AD-A238 025

MENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	29 SEP 87	FINAL REPORT

4. TITLE AND SUBTITLE
Defense Logistics Agency Computer-Aided Acquisition & Logistics Support Security

5. FUNDING NUMBERS
DLAH00-87-D-0011-0007-CDRL B004

6. AUTHOR(S)
KCH Systems, Inc

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
KCH Systems, Inc
205 South Whiting St, Suite 400
Alexandria, Virginia 22304

8. PERFORMING ORGANIZATION REPORT NUMBER
8056

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Headquarters Defense Logistics Agency
Cameron Station DLA-ZIR
Alexandria, Virginia 22304-6100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
N/A

12a. DISTRIBUTION/AVAILABILITY STATEMENT
no restrictions on availability

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

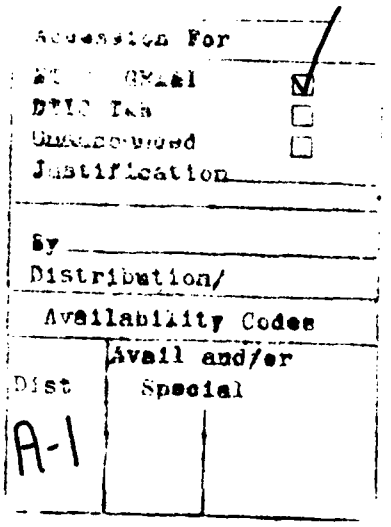
Report reviews security considerations for the Defense Logistics Agency in its participation in the Computer-aided Acquisition Logistics System. (CALS).

14. SUBJECT TERMS security, electronic security, data processing security, Computer-Aided Acquisition & Logistics Support, CALS

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
unclassified	unclassified	unclassified	



DEFENSE LOGISTICS AGENCY
COMPUTER-AIDED ACQUISITION & LOGISTICS SUPPORT
SECURITY MEASURES

UNCLASSIFIED

prepared for

Headquarters, Defense Logistics Agency
Cameron Station
Alexandria, Virginia 22304-6100

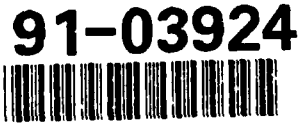
pursuant to

Contract DLAH00-87-D-0011-0007
CDRL B004

by

KOH Systems, Inc.
Systems Technology Division
205 South Whiting Street, Suite 400
Alexandria, Virginia 22304
(703) 370-4882

29 September 1989
8056



KOH

KOH SYSTEMS, INC.
Systems Technology Division
205 South Whiting Street, Suite 400
Alexandria, VA 22304-3632
Tel.: (703) 370-4882

29 September 1989
8056

Dr. Walter Simonson (DLA-ZID)
Headquarters, Defense Logistics Agency
Cameron Station
Alexandria, Virginia 22304-6100

Contract: DLAH00-87-D-0011-0007

Forwarded herewith are ten (10) copies of Defense Logistics Agency Computer-aided Acquisition & Logistics Support Security Measures (final) report pursuant to CDRL B004 of subject contract. This final report incorporates your comments and our discussions of earlier draft deliverables.

Yours truly,

C. Shumaker
Vice President

CS/dlb

cc: Ms. Faye Myers (DLA-DACO(PE))
Mr. Frank Dixon (DLA-IA)

ACKNOWLEDGEMENTS

A profound depth of gratitude is owed to Dr. Walter E. Simonson (DLA-ZID) and Mr. Frank L. Dixon (DLA-IA) for their insightful comments, critiques, and contributions during the detailed discussions of the preliminary drafts of this document.

Mr. Donald F. Blasl (DLA-IA) is also recognized for his assistance and suggestions in the research of computer security documents necessary for the development of this report.

TABLE OF CONTENTS

DEFENSE LOGISTICS AGENCY

COMPUTER-AIDED ACQUISITION & LOGISTICS SUPPORT

SECURITY MEASURES

1.0 EXECUTIVE SUMMARY

1.1 Abstract

This study reviews the security considerations for the DLA participation in CALS initiative. Its purpose is to highlight areas of concern and point out those areas to be explored for solutions to anticipated problems.

The findings are:

- *CALS data in a network of government and non-government system networks has no security focal point;*
- *the potential for inferring classified information from a vast reservoir of related, but unclassified, data is a real and present danger;*
- *the intended magnitude of unclassified CALS technical data sharing poses a security vulnerability;*
- *the nature and limit of government responsibility are not adequately defined for proprietary data that may be damaged, changed, purloined, or otherwise suffer diminished value as a result of a contractor's participation in CALS;*
- *most DoD component logistics AIS designs do not use the sophisticated software and data base environments having security and integrity features commensurate with today's needs.*

This study recommends:

- *the CALS Office promulgate policy that CALS specific training be expanded to include the inherent security implications of automated, networked, technical data;*
- *the CALS Office designate a single point of contact for CALS security;*
- *DoD CALS Office require each of the DoD components to designate a single focal point to provide interpretative, consultive, and accreditation assistance;*
- *the CALS Office discuss with ASD (C^3I) and other interested offices specific security procedures to guide CALS compliant program security administrators.*
- *AIS designers follow prescribed procedures to ensure the ultimate products of their efforts include essential integrity and security features.*
- *Government contracts incorporate memorandums of agreement to specify the limit of accessibility to proprietary data and necessary reporting procedures.*

1.2 Introduction

Over the past three decades, the use of computers and automated data processing has been expanding at an ever increasing rate. The worlds of business and Government have come to depend upon the prolific use of all tiers of computers--mainframes, minicomputers, and microcomputers. The unsatiated demands for increased productivity has caused computers to become the tool of choice of managers, analysts, and clerks alike.

The role of computers has also evolved from the stand-alone environment. Continued demands for increased efficiency and productivity have caused the increased use of networking and sharing of data among many users. Technological advancements have made possible the implementation of these shared environments. System and data base sharing now offers the seductive allure of a synergistic approach to weapons system life cycle management for industry and Government.

Private industry seeks to maximize its return on investment through efficient operations. Increased data sharing, then, will logically and necessarily continue as a means for business to reduce redundant administrative operations and improve the bottom line. The proliferation of different data formats among industries and trade groups, through, is not in the best interest of the Government. To better manage its many contractors, DoD has a vested interest in focusing this effort and encouraging the development of national standards for the exchange of automated technical data. Such national standards will be developed by the industry-Government joint venture--Computer-aided Acquisition Logistics Support (CALS) initiative.

This innovative initiative, however, must deal with accompanying complex security issues. In a stand-alone environment, security of computer systems and data is relatively easy to maintain; often requiring only physical security of the machines and the important stored data. Security of systems and data bases is more difficult in a relatively open environment of electronic transmission, reception, and manipulation of data. It is expected that this study will provide a broader discussion and fuller appreciation of the

threats to security that are a consequence of the CALS initiative.

1.3 Goals and Strategies

The Department of Defense has provided policy level guidance on the introduction of advanced computer and telecommunications technology. In 1988, OSD published the LOGISTICS 2010, Department of Defense Logistics Strategic Planning Guide. This document set the stage for massive expansions and changes in the DoD operations and logistics communities, their interactions with each other, and their interactions with industry. It set forth the Logistics Goals and Objectives along with the Strategies to achieve them through year 2010. One such Goal: *Improve the Quality of Logistics Management and Operations* was supported by the Strategy of a demonstrated CALS capability by 1994. Additionally, LOGISTICS 2010 directed that all security issues be identified by 1990 and resolved by 1995. As used in this document security refers to the protection of information from unauthorized destruction, disclosure, modification, and denial of use.

CALS is a cooperative DoD industry strategy to achieve material improvements over current paper-intensive acquisition specification and logistics support processes through the ultimate implementation of a highly automated, integrated DoD-industry environment. Its implementation is in two phases. The objective of Phase I is the definition of standards for digital information flow interfaces. This is currently ongoing. The objective of Phase II is the integration of multiple DoD and contractor weapon systems data bases. This is planned for completion by the end of 1992.

The information environment to which CALS aspires is depicted in Figure 1-1 reproduced from the December 16, 1988 issue of Software Technology Service Bulletin. The overlaying components depicted as rectangles in the data base are different data bases hosted at different sites, some by Government and some by industry. All provide collective data sharing to each other and to their users so as to maximize efficiency and minimize redundancy.

Recognizing data security as an important issue, the on-line access provisions of the Integrated Weapon System Data Base (IWSDB) has been restricted to unclassified data. Unclassified data, however, may still be sensitive, proprietary or provide the basis for

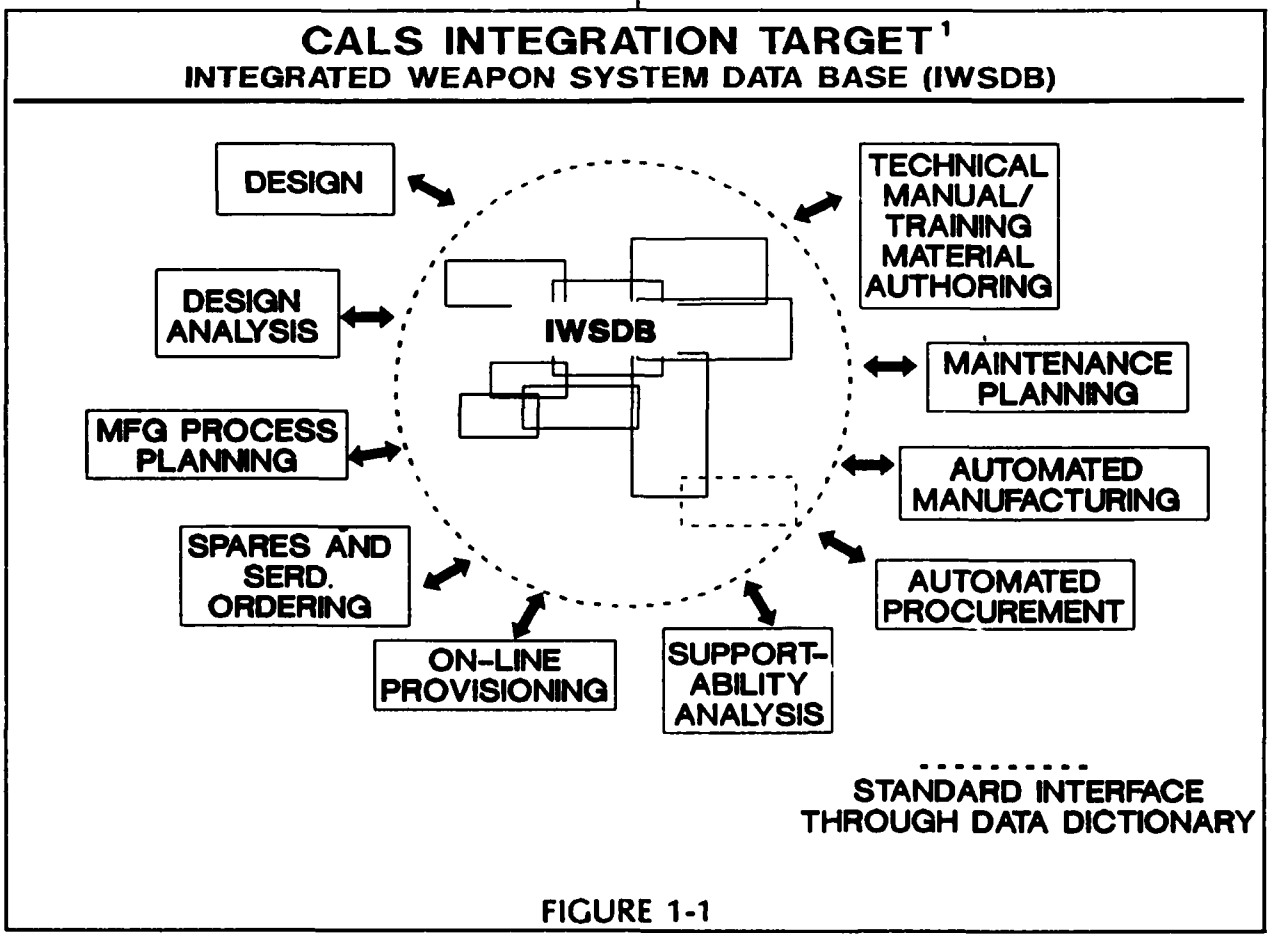


FIGURE 1-1

inference of classified data. Hence, the security issue looms as large as ever as a task to be defined and resolved.

DLA has been analyzing its needs and planning the modernization of its operations. It has adopted and promulgated a Conceptual Functional Requirements document to guide its managers in the achievement of its modernization objectives in much the same manner it was guided by LOGISTICS 2010. Whenever feasible, DLA plans to adopt on-going DoD logistics interface standardization initiatives such as CALS. It is working with other DoD components and industry to adopt additional standards for data and data exchange. It has requested policy assistance from OSD in the following areas pertinent to this study:

- Government-wide data sharing of contract data to create a single automated logical contract record for each contract to be used by both contract administration and audit personnel with eventual data input to the contractor profile.
- Increase availability of technical data through a policy of increased emphasis on purchasing required technical data, or by obtaining access to Service and contractor owned data, using CALS standard data structures.

DLA's modernization initiative has adopted a concept of maximum data sharing. DLA intends to increase accessibility of technical data by obtaining access to Service and proprietary data through electronic interfaces. Digitized technical data conforming to the CALS standards will be required as a contract deliverable. DLA will develop and maintain technical data repositories such as the Engineering Data Management Information Control System (EDMICS). EDMICS will store and transmit technical data in accordance with CALS standards. It will ultimately be available, via electronic interrogations, to the logistics functions within DLA as well as its customers and selected contractors.

Security is a major issue. Some unclassified but sensitive information requires protection for proprietary and procedural reasons. For information bearing national security classification, well-developed procedures exist for its storage and transmittal. Trusted computer *systems* are in the process of having their configuration defined and certified. Trusted computer *networks* are more difficult to specify but the effort is being made by the National Computer Security Center.

The employment of security measures must be balanced against their cost. Security measures can severely limit hardware and software options, sharing of data, and can increase maintenance costs. Hence the measure of security employed should be based on the value of what is being protected, the severity of the threat against it, and the risks associated with its participation in CALS in the light of current policy. This study is one such effort to identify and resolve security issues.

1.4 Problems - Threats to Security

In recent years there have been many examples of well publicized security transgressions against unclassified as well as classified systems. Our lexicon has been expanded to include unique definitions and connotations associated with terms such as computer virus, hacker, Trojan Horse, worm, etc. These terms have been associated with many lapses in computer security primarily due to unauthorized access to systems and data bases. The solution to most of these security problems lies in strengthening security administration.

The Defense Investigative Service/Defense Security Institute through its Defense Industrial Security Program (DISP) determined that the 10 most frequently occurring security problems can be resolved by better security administration. This is particularly revealing since the DISP focuses on data centers processing classified data. It can be expected that a similar situation exists at centers with relaxed security procedures processing unclassified data, though procurement sensitive and proprietary, such as CALS participants. A great deal of time, energy, and money has been spent thus far in developing CALS standards; and more resources need to be invested for this initiative to reach its full potential. A comparable allocation of resources must also be devoted to secure these valuable information assets.

While many problems can be resolved with better security administration this study has identified four more complex issues whose solutions are not so readily discerned. The key issues are listed in Figure 1-2.

Inferring classified data from unclassified data probably poses the most difficult issue to be resolved. In a dynamic and diversified situation such as weapon systems procurement, it is difficult to determine the many possible combinations and permutations of unclassified information data elements that may be developed much less review each for classified inference. It is certain, however, that given the broad spectrum of available weapon system data, inferring classified data is possible. How valuable is the inferred information and what level of resources support is necessary? The answers to these questions

CALS SECURITY

Key Issues

- o Strengthening Computer Security Administration
- o Inferring Classified Data
- o Managing the Magnitude of Data Sharing
- o Specifying Government Liability Limits for Proprietary Data
- o Updating Logistics AIS Designs

FIGURE 1-2

and the resolution to this issue is not readily forthcoming. It may be that all CALS data needs to be treated as classified data at the C2 level.

The magnitude of data sharing poses a dilemma for security administrators; the magnitude applies to the amount of information, number of interconnected systems, the number of users, and the geographical dispersion of all these entities. The magnitude of data sharing portends a security enigma. Many of the CALS targeted systems and data bases are currently running without the necessary security software to protect them from unauthorized access if interconnected. The established infrastructure of data processing, however, can only be replaced at substantial expense. Though this issue of expense and burden sharing between Government and industry is being addressed, it remains unresolved. While discussions continue, however, it is prudent to promulgate guidance that no new information be entrusted to systems that do not currently meet minimum security requirements.

Government liability in disseminating proprietary data also needs to be defined. CALS envisions the networking and sharing of private as well as Government data. Private data is very often categorized as proprietary. As such, it is protected by law. The Government must specify how proprietary data, incorporated in CALS, is to be protected by administrators and users. Further, the Government must clarify the limits of its responsibility for proprietary data and systems that may be damaged, changed, purloined or otherwise suffer diminished value as a result of participation in CALS.

Most of the current DoD component logistics AISs in production were designed and implemented in the sixties and seventies, prior to the availability of sophisticated software and data base environments having security features commensurate with today's needs. Nor was there great concern for the security of unclassified data processed in these systems when they were implemented; greater concern and emphasis were accorded operating efficiency and user needs (friendliness). In the eighties, all DoD components have undertaken major redesigns and re-implementations of their logistics AISs. However, none of these efforts have constituted an integrated ap-

proach to all forms of technical data as defined by CALS.

The shift to more extensive on-line processing, the sharing of data, interactively, between systems and the expansion of data to include all types and forms of representation necesesary to meet CALS objectives present AIS designers with difficulty enough. The recently re-recognized and re-emphasized need for appropriate security further compounds the designer's task, especially when the system under design is far more comprehensive than its predecessors and must be addressed in the light of its on-line interactions with other systems and communities of users.

1.5 Security Performance Measures

Whereas security standards and procedures are well defined by the National Computer Security Center (NCSC) for classified systems and data, standard performance measures for logical security mechanisms have yet to be developed. Logical security, as opposed to physical security, refers to the electronically coded logic that controls access to the computer's programming. The NCSC does evaluate and assign a rating to logical security products but there is no organization or system follow-up to assure that program participants are employing them. To ensure the integrity of all data bases and systems incorporated in the CALS initiative each participant in a CALS-compliant program has a vested interest in applying the published standards and guidance for security in unclassified data processing. The published standards and guidance do not provide specific security performance measures but do provide the basic tenets for implementation of a security program.

1.6 Current Relevant Security Initiatives

Well publicized illicit and unauthorized computer penetrations during the last decade have served to heighten security awareness and instigate deliberate action to better protect valuable system and data resources. The DoD established the NCSC in 1981 to advance the widespread availability of trusted computer systems. The function of the NCSC is to evaluate technical protection capabilities of industry and Government developed systems in accordance with published standards. These standards are promulgated as DoD Trusted Computer System Evaluation Criteria.

The Congress passed the Computer Security Act of 1987. This law defined sensitive data and focussed the attention of federal agencies on computer security. It required the agencies to prepare and submit security plans for sensitive but unclassified systems to the National Institute of Standards and Technology (NIST). NIST has established the Computer System Security and Privacy Board to develop security standards and guidelines. It also is sponsoring and coordinating anti-virus response centers.

DoD has mandated that all DoD-component automated information systems processing sensitive unclassified information must achieve classification level C2 by 1992.

The DoD CALS Office has impaneled an Industry Steering Group for Data Protection and Integrity to assist in clarifying security issues and developing guidelines for participants in weapon system programs employing CALS.

1.7 Findings and Recommendations

Each of the initiatives listed above helped advance the security aspects of automated data processing. However, the introduction of widespread system and data base sharing among Government, industry, academia and individual consultants demands new administrative and security controls. Additional policy guidance and publication of standard procedures to ensure the integrity and safeguard the valuable system and data resources must be promulgated.

1.7.1 Findings

While this report has used numerous references to recently published penetrations of public and private systems to focus the readers' attention on system security, and integrity issues, these are but symptomatic of past and present systems management shortfalls. New system security initiatives have been taken by DoD and NIST; and industry is responding with new products. However, the CALS initiative is such a far reaching concept that one is immediately awed by the magnitude of the potential security problems ahead. Four areas of concern are the inescapeable conclusions or findings of this study.

1.7.1.1 Security Administration

Numerous cases of unauthorized access to computer systems have been recently publicized. Several of these celebrated events have received such notoriety and press coverage that they have focused attention on computer security. This has led to the publication of additional policy guidance within the Government, and the introduction of legislation in the Congress. However, there is still but limited importance and resources accorded security for Government systems employed for processing unclassified and unclassified but sensitive and proprietary data. This is especially relevant to CALS. There is no single point of

contact to publish standard operating procedures, provide training, conduct inspections, answer questions, or resolve issues for participants in CALS compliant weapon systems programs. Whereas Government sites have designated security administrators, CALS data, in a network of Government and private system networks, has no security focal point.

The lack of a network security focal point compounds the problem of effective security administration since there is no means to enforce the guidance and standards that do exist. The Defense Investigative Service/Defense Security Institute has determined that the ten most common occurring security mistakes are non-technical in nature and can be corrected with increased management attention to security. As summarized in MIL-HDBK-59, this task is obviously beyond the capabilities of DoD weapons system acquisition program offices.

1.7.1.2 Inferring Classified Information

The most troublesome issue is the most ill defined. The potential for inferring classified information from a vast reservoir of related but unclassified data is a real and present danger. Real because it can now be accomplished. Dangerous because the universe of potentially inferable classified information is indeterminate. The number of possible combinations and permutations of technical data that could constitute classified information may be too numerous to effectively adjudge. Each must be reviewed individually and continually because of the dynamic aspects of both the interconnected systems and the external factors, such as political, economic, and legal, that impinge upon weapon system procurements and life cycles. It is certain, however, that given the broad spectrum of currently available weapon system data in various media, inferring classified information is possible. The higher degrees of technical data automation implicit in CALS only enhances one's ability to draw classified inferences. How critical might be the inferred information and what commitment is appropriate to preclude inference? Each weapon system implementation of CALS will require numerous and separate assessments and determinations. The answers to these questions and the resolutions to these issues are not readily forthcoming.

1.7.1.3 Magnitude of Data Sharing

The intended magnitude of unclassified CALS technical data sharing poses a security vulnerability. The number of systems exchanging data, the number of users that will have access, and the geographical dispersion of systems and users are potentially random in propogation. The protocols, formats, and rules for interchanging data are publicly evolving. Each of these aspects impacts on security administration. Many of the potential CALS data host systems are probably now running without the necessary security software to protect them from unauthorized access (no one knows) and may be incompatible with available security software. The in-place infrastructure of Government and non-government data systems, however, can only be replaced at substantial expense. Though this issue of expense and burden sharing between Government and industry is being addressed, it remains unresolved. While discussions continue, however, it is only prudent that the implementation of CALS by weapons system program offices should proceed cautiously.

1.7.1.4 Government Liability for Proprietary Data

CALS envisions the networking and sharing of private as well as Government data. Private data is very often categorized as proprietary. As such, it is protected by law. Now proprietary data shall be trusted to the administrators of the various contractor and Government systems participating in a weapon system's life cycle. The nature and limit of Government responsibilities in such environments are not clearly defined in FAR or DFAR for contractor proprietary data and systems that may be damaged, changed, purloined or otherwise suffer diminished value as a result of a contractor's participation in CALS.

1.7.1.5 Antiquated Logistics AIS Designs

Most of the current DoD component logistics AISs in production were designed and implemented in the sixties and seventies, prior to the availability of sophisticated software and data base environments having security features commensurate with today's needs. Nor was there great concern for the security of the unclassified data processed in these systems when they were implemented; greater concern and emphasis were accorded operating efficiency and user needs (friendliness) as these were the first major implementations of logistics systems having extensive on-line files of data. However, very little of this data was other than accounting, application, and supply inventory data. The predominant mode of processing was batch due to the large proportion of MILS transactions and the capabilities of supporting telecommunications services.

In the eighties, all DoD components have undertaken major redesigns and re-implementations of their logistics AISs. However, none of these efforts have initially constituted an integrated approach to all forms of technical data as defined by CALS. Most of

the major logistics systems development programs now underway were undertaken prior to the advent of the CALS initiative. They have, however, all been predicated upon the advantages to be gained through more extensive use of interactive processing techniques by using current data base management systems and advanced software tools.

On average, these efforts are three years beyond schedule and have experienced major cost growth.[2] In none of the cases reported upon by the GAO has the difficulty in achieving system and/or data base security goals been cited as a cause for developmental delays or cost overruns.

The shift to more extensive on-line processing, the sharing of data, interactively, between systems and the expansion of data to include all types and forms of representation necessary to meet CALS objectives present AIS designers with difficulty enough. The recently re-recognized and re-emphasized need for appropriate security further compounds the designer's task, especially when the system under design is far more comprehensive than its predecessors and must be addressed in the light of its on-line interactions with other systems and communities of users.

1.7.2 Recommendations

On the basis of the survey and distillation of issues germane to CALS and ADP/T systems security which have been summarized in preceding sections, three areas of improvement in security emphasis are deemed appropriate; they are: security administration, AIS design and contractor proprietary data. The first, security administration, is equally appropriate to currently operational AISs and could lead to near-term improvements in security. The latter two, AIS design and contractor proprietary data, are more long term in perspective and are essential security measures as implementations of CALS evolves. Specific recommendations applicable to each of these three areas follow.

One specific issue does not fall within the bounds of these areas and requires separate policy level research for the guidance of all participants in CALS. The Freedom of Information Act (Title 5 United States Code, Section 552, see DoD Directive 5400.7), the Export Control Act (PL 90-629, see DoD Directive 5230.25) and the DoD Directive 5230.24, Subject: Withholding of Unclassified Technical Data from Public Disclosure, seem to represent opposing views which compound the confusion of DoD and DLA systems analysts. It is recommended that the CALS Office request clarification of the intersection of these three DoD directives as they impact upon CALS technical data sharing from the Office of the General Counsel.

1.7.2.1 Security Administration Recommendations

It is recommended that DLA make the following recommendations to the DoD CALS Office to ensure improvements in systems security administration by all participants in the implementation of CALS concepts:

(1) DoD CALS Office pursue the promulgation of policies to incorporate CALS-specific security implications in the curricula of all DoD technical and management training programs.

(2) The DoD CALS Office designate a single point of contact for security.

(3) DoD CALS Office require each of the DoD components to designate a single focal point to provide interpretive, consultive, and accreditation assistance to: its acquisition program office contracting officers, and security officers; Government AIS design/development personnel and host-site ADP security administrators; and, industry/contractor host site system security and data base administrators.

(4) DoD CALS Office discuss with ASD (C^3I) and other interested offices specific procedures to guide CALS participants in areas such as:

(a) Requiring each host-site have a security administrator that has completed an accredited ADP security course before that site can be connected to a DoD component data network. A host site is defined as a Government or Government-sponsored site that stores CALS technical data on-line for access by its local users and other remote users.

(b) Requiring each host site supporting CALS technical data to administer, for its own protection, a security program to limit access to unclassified, sensitive, and proprietary data on a need-to-know basis for its indigenous users, and to closely manage, monitor and report upon accesses by external (e.g. remote, other organizations) users having access to such technical data.

(c) Requiring that each host site coordinate the granting of remote access privileges to a user (user group) with the ADP security administration of the user's/group's host site prior to granting any access.

(d) Requiring each host site to validate, at least annually, the integrity of its on-line CALS technical data by auditing it for unauthorized and in-

advertent modifications. Government site certifications should be submitted to the DoD component support center (see (3) above) with a copy to the sponsoring weapon system acquisition program office(s). Government-sponsored site certifications should be submitted to the Administering Contracting Officer with a copy to the sponsoring weapon system acquisition program office.

(e) Requiring that each host site supporting CALS technical data report, at least monthly, the number of confirmed and suspected attempted and successful penetrations of systems and data bases (by type of data: (unclassified, sensitive, proprietary) and user (indigenous or remote)) to the sponsoring acquisition program office(s), with advance copies to the DoD component support center and the DoD CALS Program Office.

(f) Denying CALS participation to contractors having systems and data bases which do not meet defined with minimum security standards.

1.7.2.2 **AIS Design Recommendations**

Department of Defense Directive 5200.28 establishes mandatory, minimum Security Requirements for Automated Information Systems (AISs). It requires that unclassified information and sensitive unclassified information be safeguarded. While it does not specifically address unclassified proprietary contractor data which is to be automated and shared pursuant to CALS, it can be assumed that such data should be accorded at least the same treatment as sensitive unclassified information. All DLA and DoD AIS designers must comply with the Directive, and other official regulations and guidance, cited therein. Once an AIS designer determines the AIS being addressed will involve the processing of sensitive and/or proprietary unclassified data, it is recommended that they consider the steps below to ensure the ultimate products of their efforts have essential integrity and security features incorporated in their infrastructures and operational interfaces.

1. Do not assume a host environment meeting class C2 security requirements is sufficient to meet all AIS security needs; assume that the C2 defenses can be penetrated.

2. Confront functional sponsors to specifically define the full range of security and integrity aspects of their business operations being automated, or re-automated, by the AIS. Place special emphasis on determining what inferences may be drawn from data internal to and about their operations when combined with information/data from other sources.

3. Force the functional sponsors to define and categorize each type of user of AIS services or products, by type of organization and/or organizational echelon, as to their need-to-know classification by data topic.

4. Prepare a statement of AIS security requirements, for approval and acceptance by the functional sponsor, which defines the accessibilities and controls of each category of user.

5. Codify every element of data to be accessed, processed, stored, and maintained by the AIS as to its classification, sensitivity and proprietary nature. In addition, determine what other types or elements of data they may be combined with to yield (infer) classified, sensitive or proprietary information. Validate these codifications and relationships with the functional sponsor.

6. Expand the codification of data elements to record the accessibility to be granted each type of user (both internal and external to the target organizations) and the form (on-line or printed output only) of access.

7. Once the process/transaction flows and supporting data requirements have been conceptualized, classify each data interface and user interface, as to its source(s) of protective mechanisms (e.g. communications access, operating system, application, data base management system).

8. Partition the AIS modules and data bases, to segregate users having differing needs-to-know and employ interim DBMS security protection features to safeguard sensitive data and/or combinations of data internal to the AIS.

9. Eliminate any internal AIS access/transfer linkages which can assume a disparate access authority; ensure all user and program directed branches pass control to the entry points of paths having integral application and/or DBMS security checks.

10. Test the AIS's security logic design to batch and interactive natural (e.g. fourth generation) and ad hoc (e.g. on-line structured query) language interfaces.

11. Specify what internal AIS features will be incorporated to report attempted penetrations of its programs, parameter tables or data bases, and to whom these reports shall be addressed; these are in addition to host systems-level telecom-

munications and operating system software reports.

12. Test the integrity logic of the AIS design by validating its immunity to deliberate, inadvertent and accidental (e.g. system crashes) changes in inputs, parameters, data bases and outputs.

13. Specify what measures, to be used on what cycles, are to be employed to validate the integrity of the AIS computer programs and data bases and to detect unauthorized and/or uncertified changes.

14. Test the security and integrity logic of the AIS design by group walk-throughs of each batch and interactive transaction through each AIS module with the functional sponsor; test for the inference of classified, sensitive or proprietary information, at each point the AIS produces an output product (hardcopy, inter-AIS transaction, or workstation user display).

15. Carry out, re-validate and specifically test the security and integrity designs during each phase of the AIS development, initial operational test (IOT), and deployment process.

16. Conduct a distinct and separate test of the AIS's security and integrity with the functional sponsor, Information System Security Officer (ISSO) and host site System Security Administrator for the purpose of accrediting it prior to placing it in operation at an IOT or follow-on site.

17. For each functional and remedial maintenance change throughout the life cycle of the AIS, reiterate steps 2 through 16 above for validation purposes.

When the requirements analysis, design and/or development of an AIS is contracted out, the contractor should be contractually obligated to employ comparable methods to those outlined above to achieve appropriate security and integrity. Since such a contractor would be much less knowledgeable or aware of the potential for classified inferences from unclassified aggregations, the Government should very thoroughly validate the contractor's deliverables.

1.7.2.3 Contractor Proprietary Data Recommendations

Heretofore, when the Government has furnished the proprietary data of one contractor to another it has been in a hardcopy media and in accordance with specific contract clauses and FAR/DFAR. Through CALS, the Government shall be providing all contractors direct access to its systems hosting contractor-provided proprietary data and authorizing other contractors to access the proprietary data of a contractor hosted on its own system, but made available pursuant to one or more Government contracts. Whereas under earlier practices, contractors providing and receiving data were both protected by, and subject to, numerous rights in data FAR/DFAR regulations and statutes, the CALS sponsored network of data systems environment introduces new and more difficult accountability issues. MIL-HDBK-59 leaves individual weapons systems program managers and contracting officers to work the details of each arrangement. The proper medium for such arrangements are contracts which incorporate the memorandum of agreement (MOA) required by DoDD 5200.28. It is recommended that these MOAs include the following:

1. Contractor and Government users should only be granted read-only access to the proprietary data of a contractor whether hosted on a contractor or Government system;

2. Contractors providing on-line access to their own proprietary data shall provide the Government a monthly report of each Government and other contractor user access to the data in much the same manner as timesharing companies invoice their customers (i.e. user ID; data-time-duration of access, programs employed, data sets accessed);

3. Government systems hosting contractor proprietary data shall provide monthly reports to the owning contractor(s) of accesses to its data by other contractors.

The DLA should recommend to the DoD CALS Office that it should research, adopt and promulgate standard data elements and formats for the reporting schema recommended above, so they may be exchanged in digital form.

1. Computer-aided Acquisition and Logistics Support (CALS), *Software Technology Service Bulletin, 16 December 1988, IDC Washington, Inc., Vienna, Virginia*

2. Report to the Chairman, Legislative and National Security Subcommittee, Committee on Government Operations, House of Representatives, Automated Information Systems, Schedule Delays and Cost Overruns Plague DoD Systems, *United States General Accounting Office, May 1989, Washington, D.C.*

2.0 CAPITALIZING ON TECHNOLOGY

This study reviews the security considerations for the DLA participation in the Computer-aided Acquisition and Logistics Support (CALS). Its purpose is to highlight areas of concern and point out those areas to be explored for solutions to anticipated problems. It is expected that it will provide a broader discussion and fuller appreciation of the threats to national security the fruition of this initiative could present.

The purpose of this section is to summarize these general stimuli for change as viewed by the Department of Defense via its policy level guidance on specific initiatives, and as viewed within the Defense Logistics Agency.

2.1 Stimulus for Change

Advances in computer and telecommunications technology have opened doors of opportunity for a wide range of government and industry automation initiatives. On the one hand, the reduced, and continually declining, costs of computer processor power, storage capacity and data transmission have made viable the automation of processes and data collections not previously economically justifiable. On the other hand, new technologies (e.g., optical disk storage, data scanning wands, etc.) have now made technically feasible the automation processes and data collections previously unsupportable with then existing technology. As the information technology field has expanded and matured, the development of computer systems software and tools have likewise greatly expanded the technological and economical horizons of users at all levels.

The Department of Defense logistics community, an early user of computers (and their predecessor electronic accounting machines) for bookkeeping and inventory accounting data processing, is now preparing to capitalize upon these advances in technology by expanding its definition of "data". Heretofore, data has typically meant the numeric quantity on-hand, due-in, back-ordered, etc., the identity of requisitioners and suppliers, the codified applicability (end-use) of a piece part, and, of course, the dollar values associated with assets acquired and operations. Hereafter, in DoD the term "data" shall also include all textual and graphic (e.g., specification drawings) documents associated with the research, design, test, acquisition, operation, in-service engineering and disposal of weapon systems, weapon platforms, support equipment and consumables, as well as all of, and more of, the codified data now being processed.

The universality of reliance upon advancing information technology in Government and industry (and the continuing evolution of hardware interfaces, software functions, and telecommunications interfaces and protocols) have also made feasible the automation of electronic data exchanges between Government and industry participants, and the sharing of data without necessitating its replication. Such exchanges and sharing potentially offer both economies in operation and increased functionality to all participants.

2.2 Logistics 2010 Project

The Assistant Secretary of Defense (Production and Logistics) chartered the Logistics 2010 Project in August 1987 to develop logistics strategic planning guidance for all components of the DoD. In 1988 OSD promulgated the LOGISTICS 2010, Department of Defense Logistics Strategic Planning Guide. The following paragraphs contain excepts from this document which set the stage for massive expansions and changes in the DoD operations and logistics communities, their interactions with each other, and their interactions with industry. These excerpts have been selected on the basis of their probable impacts of increasing the extent of data automation, data sharing, interactions between systems and data accessibility. They are intended to convey a sense of the magnitude of the increased automation and telecommunications envisioned, and the security implications implicit in such an expansion.

2.2.1 Problems and Challenges

"The DoD's logistics information systems and command, control, and communication (C^3) systems are often viewed as peacetime systems which may have insufficient surge capacity under wartime conditions. Considerable deficiencies exist in the automation of paper-intensive and manual processes, the development of analytical tools, data security, integration and interoperability of data bases and systems.....ineffective integration within DoD and with industry." "Shared data bases, electronic interchange, common data dictionaries and standards are essential for the integration required."

"The advent of massive data bases and the employment of rapid telecommunications and international standards for describing objects and communicating status [will] make more flexible support options viable."

"Presently, the system is too frequently separate, with many islands of automation that must be integrated to significantly improve logistics decision making."

2.2.2. **Assumptions**

"Logistics and information assets will become more vulnerable as adversaries also apply technology and the information explosion increases through automation and integration."

"High cost, and consequent limited availability of key logistics assets, will dictate increasing dependency on uninterrupted logistics communications systems. Development of backup systems and alternatives that maintain and enhance critical capabilities will be imperative."

"Economic interdependencies will cause the U.S. to use more systems and technologies developed outside the United States and to rely more on international sources for equipment, supplies and support. The use of concepts such as Host Nation Support Agreements, joint ventures, and co-production will increase."

"Pressure will increase to develop and implement common and effective international standards for communicating transactions, material description, and quality and accounting information for material at all stages of production."

"The transfer of digital manufacturing information will diminish the need to transport items. As transportation, rather than storage, increasingly becomes the prime contributor to the DoD's ability to deliver material on time, the importance of inexpensive international tracking and control systems will become paramount."

2.2.3 **Logistics Objectives and Strategies**

"Problems within the current logistics system and assumptions about the future determine the areas that the DoD needs to direct attention during the next several decades. Together they provide the basis for the objectives and strategies established to achieve the mission and goals of the logistics system."

"Many strategies have common themes, and some strategies help achieve more than one goal or objective, particularly in the areas of quality, information and communications systems, and research, development and technology infusion."

Figure 2-1 from Logistics 2010 is included to summarize its goals and objectives. Subsequent pages excerpt selected strategies in support of these goals.

2.2.3.1 **Goal I - Strategies**

"By 1995, OSD, JCS, and the Components develop and implement an interoperable system for worldwide intransit visibility of material."

"OSD and each Component continue to develop and implement intermodel transportation systems and standards to increase interoperability for equipment and logistics information systems."

"By 1990, OSD issue guidance to the Components for modernizing logistics information and communication systems to include: the current functional and technical architectures for DoD; interfaces with industry and our allies; assessment of needs to support the future functional environment; a technology forecast; and a transition strategy. By 1991, Components develop plans to implement guidance."

"By 1995, OSD, JCS, and Components improve logistics command, control, and other automated systems to support crisis and contingency operations. Ensure adequate procedures and backup systems are available for continuity of operations."

"OSD and the Components examine use of commercial and other communication networks to improve capacity."

"OSD and the Components focus research and development programs on improving automated data processing (ADP), e.g., hardware/software transportability; expert systems/artificial intelligence applications; improved training aids; integrated, distributed data base management; standards; and data dictionaries."

"Components increase use of automated tools for design, programming, and data dictionaries."

"By 1995, OSD and the Components expand adoption/adaptation of commercial tools, software, hardware, and support practices that increase use of commercially-maintained data bases and systems."

"OSD and the Components maximize real-time electronic interfaces through the integration of logistics systems within DoD and with industry and our allies."

"By 1990, OSD and the Components identify logistics data security issues for data base access, transmission, and aggregation; and resolve issues by 1995."

"OSD, JCS, and each Component increase logistics data integrity through greater automation of input screens, edit and logic checks, and transmission."

"By 1990, JCS and the Components develop the capability to match the specific logistics requirements of CINC operations plans with existing resources. Focus on interoperable automated processes and data bases."

Logistics 2010 Goals and Objectives

SUMMARY

Mission

Ensure Quality Logistics Support to the Total Force for the Full Spectrum of Operating Scenarios

GOAL I: ENSURE OPERATIONAL LOGISTICS SUPPORT TO MEET READINESS AND SUSTAINABILITY REQUIREMENTS

OBJECTIVES

1. Improve inter/intratheater mobility capabilities for mobilization, deployment and resupply.
2. Field improved logistics information, command, control and communication systems for operational and logisitics managers to provide responsive decision support.
3. Improve peacetime and wartime materiel and support.

GOAL II: ENSURE WEAPON SYSTEM AVAILABILITY

OBJECTIVES

1. Increase quality of weapon system support by achieving or exceeding established logistics support goals such as reliability, maintainability, durability and interoperability.
2. Incrementally and markedly reduce the response times for initial and follow-on logistics support (e.g., weapon system acquisition, procurement lead-times, repair times, and order and delivery times).

GOAL III: IMPROVE THE QUALITY OF LOGISTICS MANAGEMENT AND OPERATIONS

OBJECTIVES

1. Modernize acquisition and logistics facilities, processes and interfaces among DoD Components to consider current deficiencies, changing concepts of operations and technologies.
2. Increase logistics workforce productivity.
3. Improve management of research and development and technology infusion into the logistics system.
4. Reduce logistics support costs.

GOAL IV: IMPROVE INDUSTRIAL BASE RESPONSIVENESS TO DOD NEEDS

OBJECTIVES

1. Improve preparedness plans for DoD organic and commercial industrial base surge/mobilization requirements.
2. Improve industrial base competitiveness.

FIGURE 2-1

2.2.3.2 Goal II - Strategies

"Military Services increase use of common systems and components to improve interoperability. OSD and Military Services develop standards for systems that must be interoperable. Encourage joint development, co-production, and use of commercial/standard components and equipment."

"OSD and the Components automate logistics information gathering, sharing and process flows to speed up decision making in acquisition and logistics functions."

2.2.3.3 Goal III - Strategies

"Components focus Research and Development (R&D) and demonstrate capabilities to improve acquisition and logistics interfaces through increased use of automation, shared data (knowledge) bases, and continuing evolution of standards that allow for exchange of data."

"By 1994, each Service demonstrate Computer-aided Acquisition and Logistics Support (CALS) Phase II concepts where technical data is permanently maintained by a contractor and accessed by U.S. and foreign government users. Determine infrastructure changes that will be required and begin incremental implementation of CALS Phase II throughout DoD."

"OSD and the Components expand electronic telecommunication interchange and integration initiatives within DoD, and with industry and other governments. Implement current programs such as Computer-aided Acquisition and Logistics Support (CALS), Modernization Of Defense Logistics Standard Systems (MODELS), weapon systems management, and Electronic Data Interchange (EDI) initiatives that enhance DoD-wide capability."

2.2.4 Security

Note that while Logistics 2010 recognizes data security in existing logistics systems (see 2.2.1 Problems and Challenges above) as a deficiency, it espouses more ex- pansive use of numerous ADP/T resources (e.g. automated system development tools, adoption/ adaption of commercial tools) which aggravates security considerations. They provide would-be penetrators the ability to predict system characteristics. But, Logistics 2010 also directs that all security issues be identified by 1990 and resolved by 1995.

2.3 Computer-aided Acquisition and Logistic Support (CALS) Initiative

CALS is a cooperative DoD-industry strategy to achieve material improvements over current paper-intensive acquisition, specification and logistic support processes through the ultimate implementation of a highly automated, integrated DoD-industry environment. The initiative's objective is the automation of the "generation, access, management, distribution, and use of technical data in digital form for the acquisition, design, manufacture, and support of weapon systems, ships and equipment. Incorporating the technologies of computer-aided design, engineering, and manufacturing (CAD, CAE, and CAM), its goals are to increase quality, decrease cost, and compress time schedules by considering cost, schedule, user requirements, and - from the outset - all elements of the product life cycle including manufacturing, maintenance and major overhauls. In other words: 'getting downstream information upstream'"[1]

The CALS initiative dates back to the early eighties and was conceptually fleshed-out by early 1983. However, it wasn't approved in its current form until 1985.

Whereas earlier programs and initiatives within the DoD and industry have automated independent portions of the technical data pertaining to military systems, CALS takes the next step forward. CALS is revolutionary in that, in compliance with Logistics 2010, it proposes to automate and make accessible via automated means all data to all participants directly and indirectly engaged in the research, acquisition, deployment, training, operation, maintenance and support of these systems. Such technical data shall include all information pertaining to the material composition, specifications, operating characteristics, and testing/maintenance of these systems. This data is to be shared with DoD, between DoD and industry, and between the United States and its NATO allies.

"Phase I of CALS, the definition of standards for digital information flow interfaces, is underway now. Phase 2, in which multiple DoD and contractor weapon systems databases will be integrated, is planned for completion by the end of 1992.

The first DoD acquisitions to implement CALS will be the Air Force advanced tactical fighter, the Navy A-12 advanced tactical aircraft, the Army LHX light helicopter, and the Navy V-22 Osprey tilt-rotor aircraft. All will share common avionics packages."[2]

The information environment to which CALS aspires for these programs is depicted in Figure 2-2. Note that the overlaying components depicted as rectangles in the data base are different data bases hosted at different sites, some by government and some by industry. All provide collective data sharing

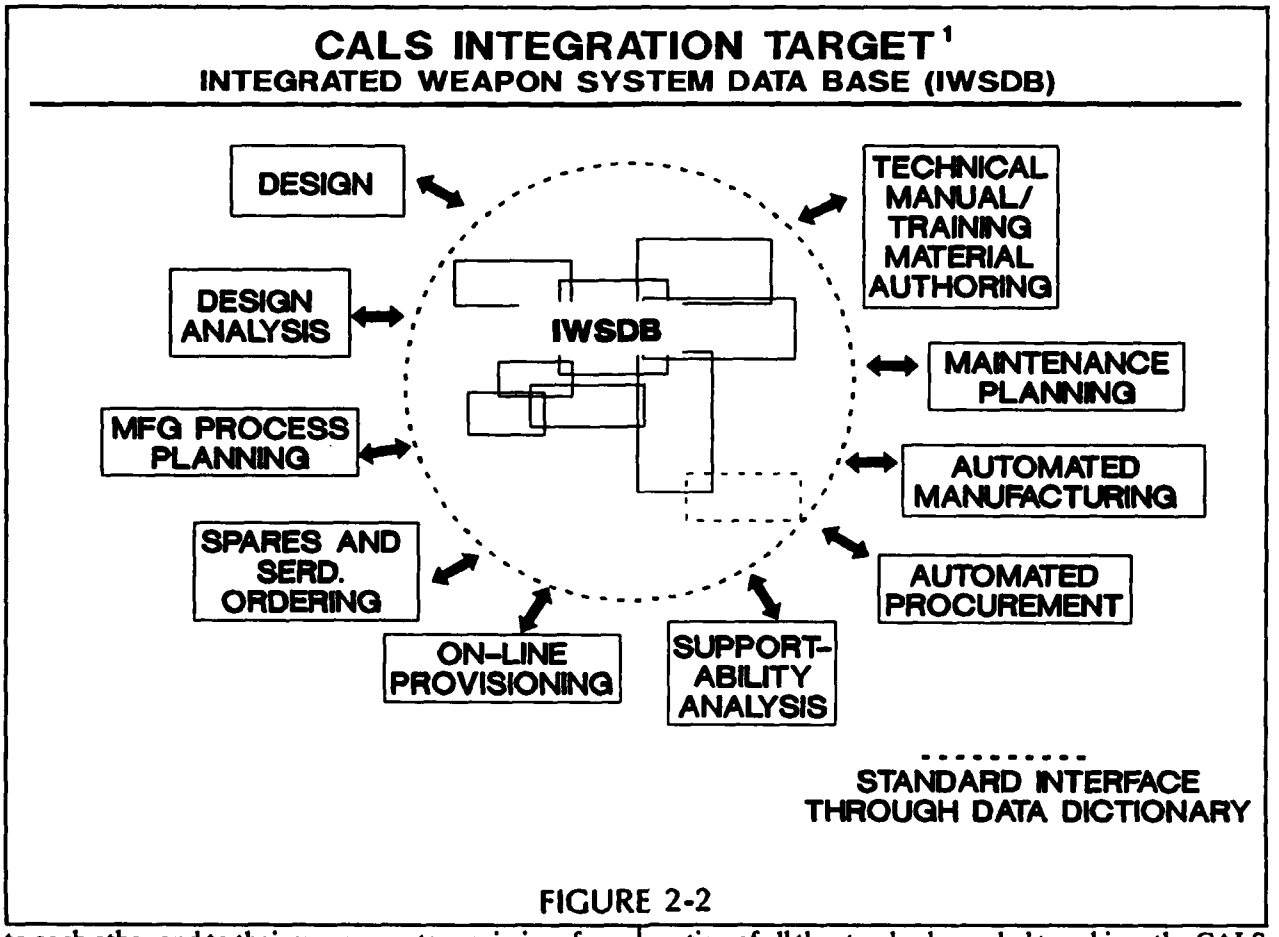


FIGURE 2-2

to each other and to their users so as to maximize efficiency and minimize redundancy.

The cornerstones of the CALS initiative are a series of standards. It is these standards, in conjunction with a series of previously adopted MIL, FIPS, ANSI, IEEE and ISO lower level standards (e.g., MIL-M-38784B, Output of Technical Data; FIPS 21-2, COBOL) which will enable the automated exchange of technical data (codified, textual and graphic) between the dissimilar workstations and host systems of the various participants in a weapons systems program. These standards were first published, including the proposed MIL-STD-1840A, on 23 April 1987 as core requirements by the DoD CALS Policy Office. MIL-STD-1840A was subsequently repromulgated on 22 December 1987. Data security was recognized in this document as an important issue requiring further definitization. Hence, the on-line access provisions of the Core Requirements Package were restricted to unclassified data. Figure 2-3 graphically depicts the topical contents of this package. Figure 2-4 reports on a typical difficulty which will be encountered by the government and industry in the formulation and effective implementation of all the standards needed to achieve the CALS environment ultimately intended.

Other CALS standards are:

"As with other software standards, the only constant is change. The Office Document Architecture (ODA) is being proposed as a mechanism to shore up the weaknesses in formatting of the Standard Generalized Makeup Language (SGML). However, a new draft standard, the Document Style Semantics and Specification Language (DSSSL) may combine the best of both with structure and style elements. The Product Data Exchange Specification (PDES) is an already planned upgrade for Initial Graphic Exchange Specification (IGES)."[1]

"ODA is expected by many to join the CALS suite of standards as are architecture for composite documents. Composite documents are those which combine source text, graphics, photographs. The many standards tailored to each type of source data require an architecture to manage this presentation to the author and user."[3]

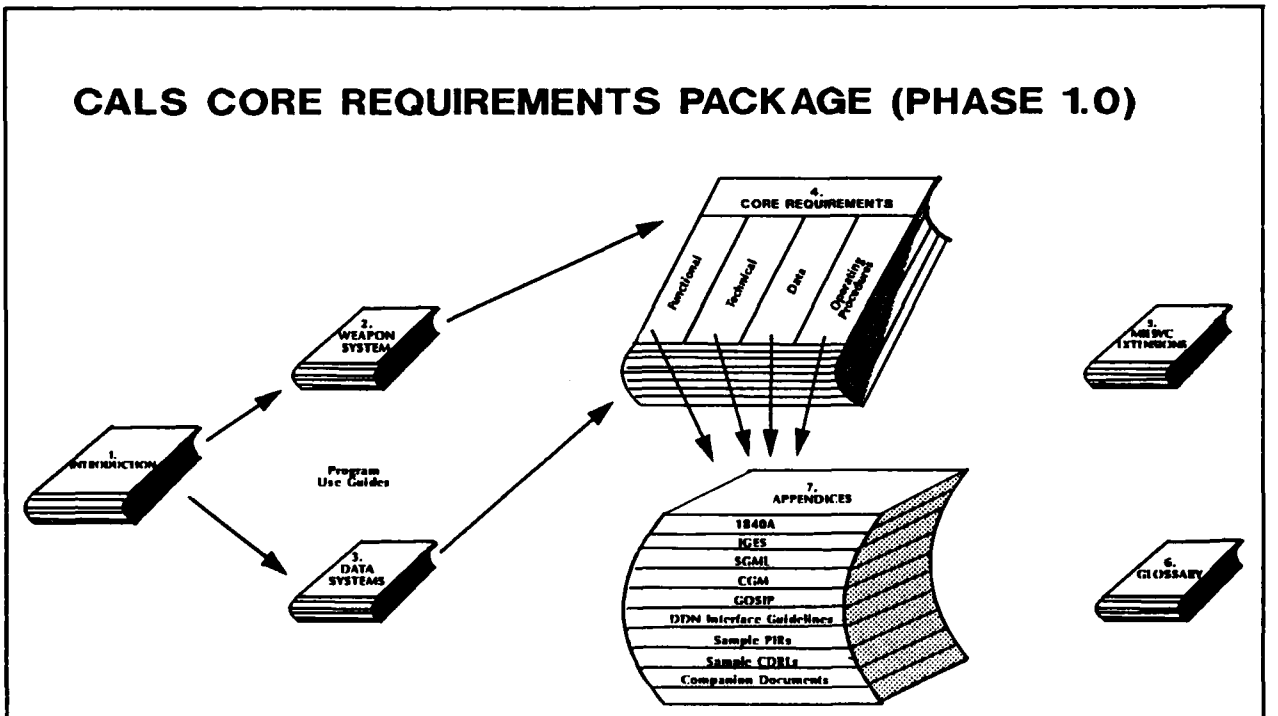


FIGURE 2-3

2.4 Defense Logistic Agency Modernization

The DLA has been analyzing its needs and planning the modernization of its operations and ADP/T systems for some time. It has adopted and promulgated Conceptual Functional Requirements to guide its program and project managers in the achievement of its modernization objectives in much the same manner as it itself was guided by OSD's Logistics 2010. Some of the changes embodied in DLA's modernization are:

- "Improved data access and expert system support, and performance measures for cost effective decision-making at all levels." (a Business Initiative)
- "Organize key data classes (i.e., those with potential for data sharing) into subject databases managed independent of the applications program that create and use them. [a Data Management Initiative]
- Research opportunities for data sharing across DLA and throughout DoD, other Federal agencies, and with industry. [a Data Management Initiative]
- Create link of customer inquiries to DLA databases to provide real-time response to queries. [a Data Management Initiative]
- Create necessary data environment to support widespread functional analysis using PCs. [a Data Management Initiative]
- Provide a current electronic image, on-line and interactive, for all participants in contract administration and review."[4] [a System Initiative]

2.4.1 Policy Support

The DLA plans to adopt on-going DoD logistics interface standardization initiatives (such as MODELS and CALS) whenever feasible, and to work with other DoD components and industry to adopt additional standards for data and data exchange. It has requested policy assistance from the Office of the Secretary of Defense in the following areas pertinent to this study:

- "Government-wide data sharing of contract data to create a single automated logical contract record for each contract to be used by both contracting, contract administration and audit personnel, with eventual data input to the contractor

Data Output Specs Need to Be Redefined, CALS Office Says

BY KAREN D. SCHWARTZ
GCN Staff

A recent test conducted by the Defense Department's Computer-Aided Acquisition and Logistics Support (CALS) office showed the current specifications for the output of technical data are outdated, according to DOD officials.

Output specifications describe all the possible renderings of the standard parts of technical documentation such as chapter headings, formatting, positioning and font size. The output specification should define rigorously all valid combinations of the various parts of the documentation, said Harvey Bingham, a lead engineer at Interleaf Inc. of Cambridge, Mass., one of the test sites for the CALS Test Network (CTN).

The CALS program is developing standards for creating, transmitting and handling computerized technical information as the data moves from industry's drawing boards to DOD agencies and then to front-line combat units.

Although CALS is oriented primarily toward weapons systems, it eventually could be used for DOD's non-weapons systems, officials said.

Deputy Defense Secretary William H. Taft IV in August directed program managers to ask contractors to include in contract bids specifications for the delivery of CALS data.

Taft said the degree to which contractors can deliver CALS data will be a factor in new awards, and he also directed program managers to review existing opportunities for using CALS.

The CTN sent identical magnetic tapes to vendors asking them to compose a document based on their interpretation of military standard 38784, which covers output specifications. Each respondent came up with a different rendering, said Al Howe, CTN's technical publications lead analyst.

Howe said the test results prove Mil-Std 38784 is outdated. "Time has passed it by," he said. "It's time to take a more definitive approach."

Michael McGrath, head of DOD's CALS office, said, "It's a confirmation of the engineering judgment that we need [new] output specifications. The benefit of the test is that it sheds some light on how tightly the output specs need to be defined to get rid of the ambiguities."

The output standards are based on International Standard (IS) 8879, which defines structure and content for technical documentation. Howe said the problem is that IS 8879 does not address format. Using IS 8879 as a basis, officials should develop a new standard that includes formatting, he said.

Larry Welsch, manager of the Office Systems Engineering Group in the Software Systems Technology Division of the National Institute of Standards and Technology, said he was not surprised at the responses, "since there isn't an [updated] output specification yet."

Welsch said new output specifications have been in the works for at least two years and a committee is defining the semantics for the new specification.

Welsch said the new output specification will be written so the services can specify which features they want to use on specific technical documents, allowing them to customize documents while still adhering to a set of defined standards.

Estimates on when a draft of the new specifications will be available for comments range from June to September.

McGrath said there are more than 150 military specifications affecting the writing of technical manuals. "The last thing we want to do is develop 150 different document type definitions [DTDs] and output specs," he said.

McGrath said officials plan to publish an initial output specification and "very carefully pick about 15 DTDs and associated output specs" that will cover the major functions.

[Government Computer News, 20 March 1989, Ziff-Davis Publishing Co., New York, New York]

FIGURE 2-4

profile. Support is needed to develop standards for DoD contractor profile. Support is needed to develop standards for DoD contract data and to ensure Service/Agency cooperation to permit contract administration personnel to read and input data to the contracting officer's records.

- Increase availability of technical data through a policy of increased emphasis on purchasing required technical data, or by obtaining access to Service- and contractor-owned data, using CALS standard data structures. This will increase our ability to make competitive purchases and will result in cost savings. In related policy for technical data, DLA will continue to promote the use of DoD standards for digitized technical data, to assure accessibility and transportability."[4]

2.4.2 Data Sharing Concept

The DLA's Modernization initiative has adopted a concept of maximum data sharing, both of its data with others and that of others with the DLA. It has appropriately recognized that "although there are many technical and institutional obstacles to overcome in achieving a data sharing environment, data sharing has far more benefits and fewer technology impediments than trying to standardize applications software across the DoD or Federal Government."[4]

2.4.2.1 Technical Data

Figure 2-5 portray's DLA's concept of technical data sharing. "Technical data for logistics includes technical manuals, procurement technical data packages, product definition data in the form of manufacturers' catalogs and specifications, engineering drawings and computer-aided design data. DLA's ability to support customer requirements is directly affected by the availability of adequate descriptive and technical information about the item to be supported.

DLA intends to increase accessibility of technical data by obtaining access to Service and proprietary data through electronic interfaces. Digitized technical data conforming to the Computer-aided Acquisition and Logistics Support (CALS) standards will be required as a contract deliverable. DLA will develop and maintain technical data repositories (such as the Engineering Data Management Information Control System [EDMICS]) that will store and transmit technical data in accordance with CALS standards. EDMICS data will ultimately be available via electronic interrogations to the logistics functions within DLA

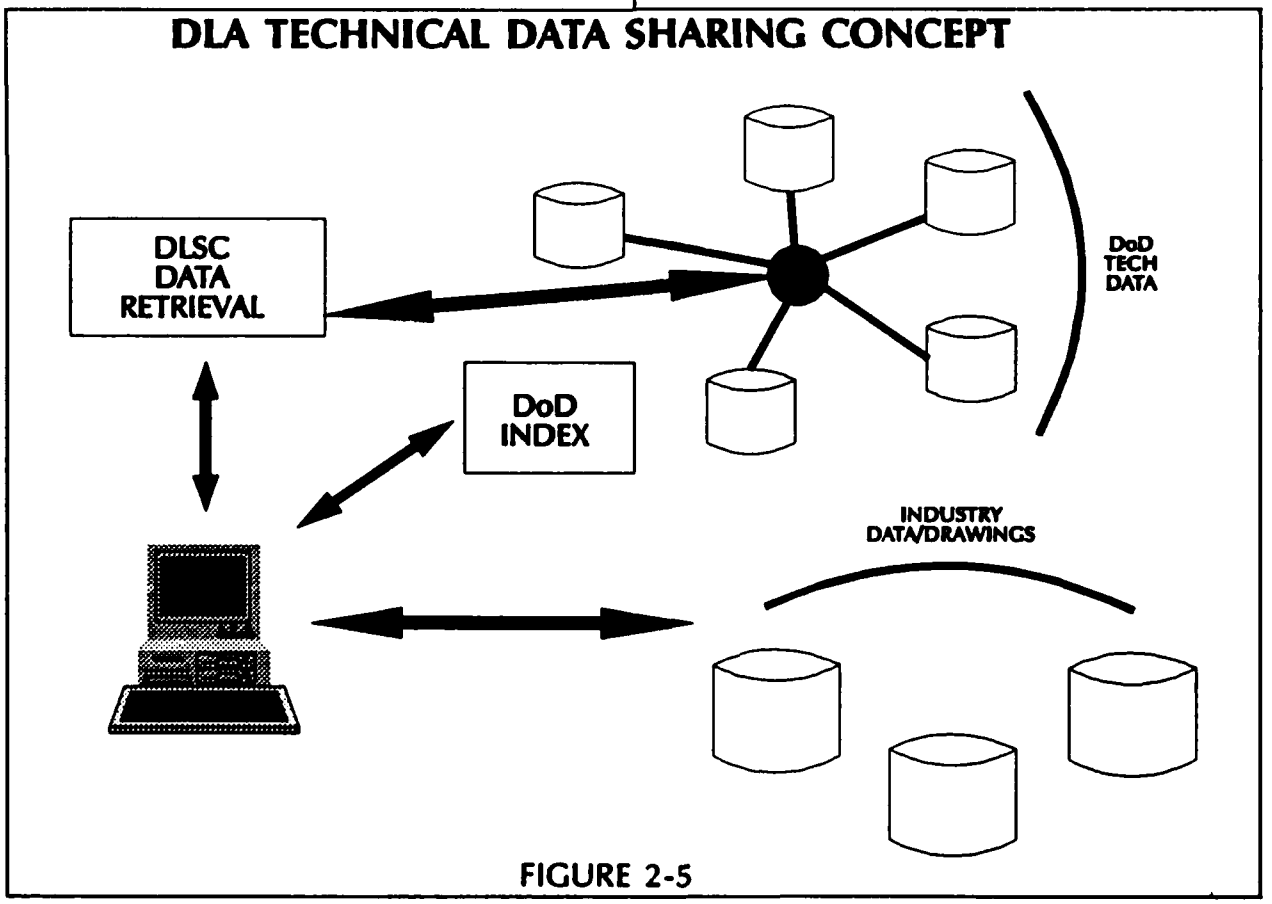


FIGURE 2-5

from procurement through disposal, as well as to DLA's customers and selected contractors.

DLA will increase the visibility of where technical data resides in the DoD by establishing a DoD index of technical data, which will cross-reference drawings and part numbers to the applicable DoD repository where the information is located. This system, entitled the Military Engineering Data Asset Locator System (MEDALS), will be immediately accessible via electronic interrogations. Ultimately, it is envisioned that MEDALS will not only indicate where the data is located, but will be able to pull and display data upon demand."[4]

2.4.2.2 **Asset Data**

"The required capability is for the item manager to maximize visibility of excess assets, in-transit inventory, due-ins from contractors and repair, industry assets and retail stocks. This asset visibility includes stocks held by activities responsible for the supply/ resupply of a maintenance activity or an operational activity but excludes stocks in the hands of ultimate users and activities such as combat ships and operational units....DLA plans to develop the capability to access DLA asset information and provide it to all DLA personnel who use it."[4]

2.4.2.3 **Contractor Data**

Consolidated and accessible historical data pertaining to DoD contractors "would provide complete contractor performance profiles to give managers a single source of data to assist in the decision-making process for awarding a contract....The profile will include information on contractor's performance from the entire procurement community including DCAA and non-DoD Government agencies. Figure 2-6 portrays DLA's concept of the sharing of historical contractor profile data. The following is a list of potential benefits:

- Contractor performance profiles will be utilized by procurement personnel to determine the responsibility of potential contractors and reduce the need for informal pre-award surveys.

- Price/cost data to perform complete analyses of contractors' price/cost proposals.

- Additional information related to product pricing will increase the probability of contracting offices negotiating fair and reasonable prices for noncompetitive procurements.

- The ability to accurately determine a contractor's delivery history for a product or similar class of

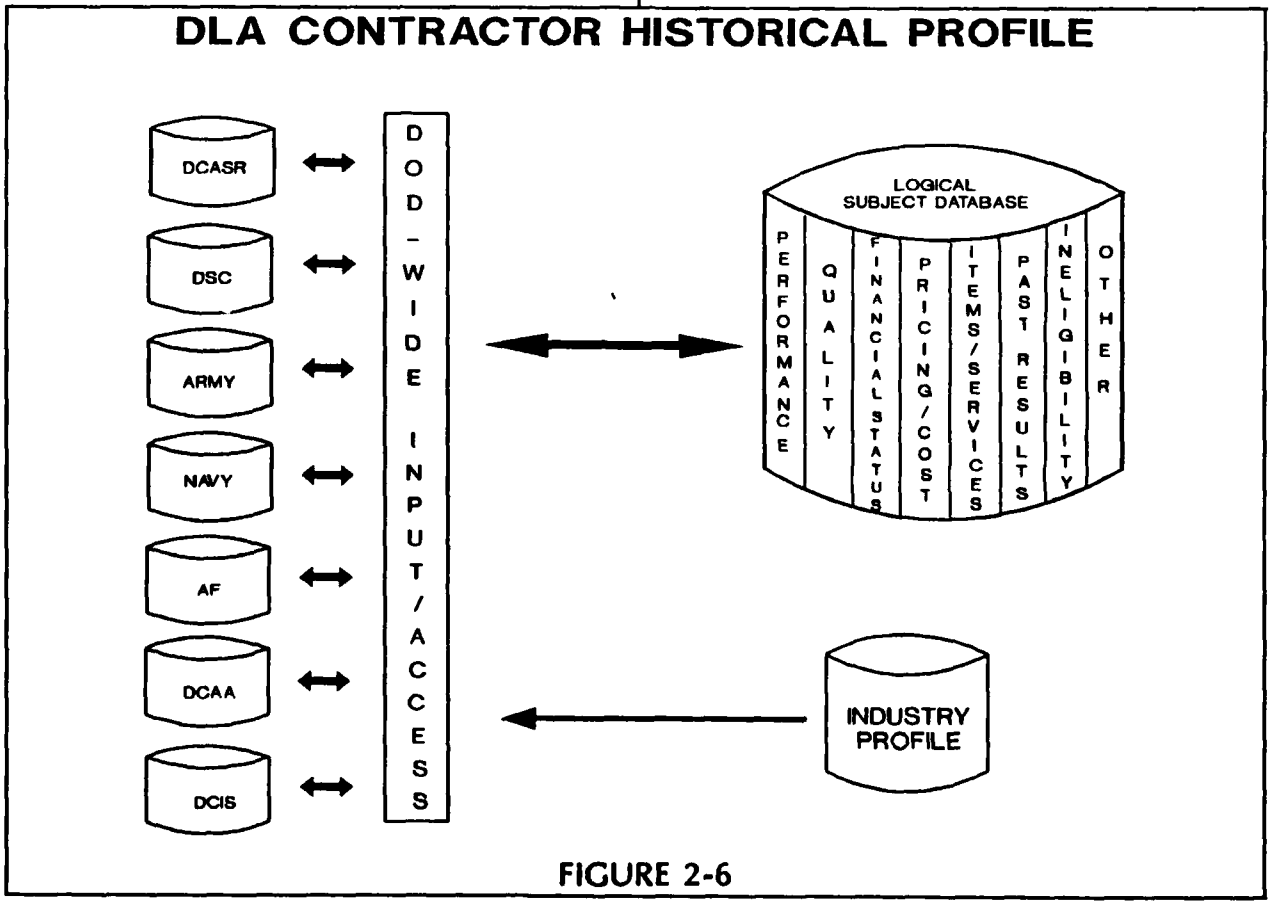


FIGURE 2-6

products will allow item managers to better select suppliers and control their inventories."[4]

2.4.3 Total System Solutions

The DLA has also put forth two total system concepts which portend the ultimate total integration or internetting of DoD and industry business information systems. It concluded that "in the course of reassessing the Agency's business requirements, DLA needs to pursue DLA-wide and DoD-wide solutions to logistics problems. DLA modernization recognizes that, for DoD to fully benefit from modern technology and information management techniques, DLA systems must be interoperable not only within DLA, but must also be able to communicate and interface with Services' logistics systems, as well as those in industry, GSA, and other Federal agencies. OSD recognition of the need for common solutions and interoperability has fueled such approaches as the Military Standard Logistics Systems (MILS) and the single manager concept. More recently this is reflected in such DoD initiatives as MODELS, CALS and EDI, which promote standardization of policies, procedures, and practices in the interest of DoD-wide efficiency and effectiveness. In some cases, when the policy effect of standardization can be achieved through the use of the technology (e.g., gateway translation of data between DoD components, or between DoD and industry) without actually standardizing procedures and practices, that course of action may be an interim solution, or may take the place of investment in system design changes to achieve standardization. Similarly, interoperability achieved through technological capabilities (such as the ability of DLA to access data held by the Military Services or industry without replicating databases, to make informed supply support decisions) will lessen the necessity for standardization of design and common equipment."[4]

2.4.3.1 Electronic Contract Instrument

Figure 2-7 portrays DLA's concept of an Electronic Contract Instrument. "Contracts are written to reflect agreements made with contractors to procure items and services. In addition, a major function of a contract is to authorize payments to those contractors. These contracts are continuously reviewed to manage, modify, and determine the status of the agreements.

The Electronic Contract Instrument concept will allow users to quickly locate contract information. This information will be used to manage, modify, pay,

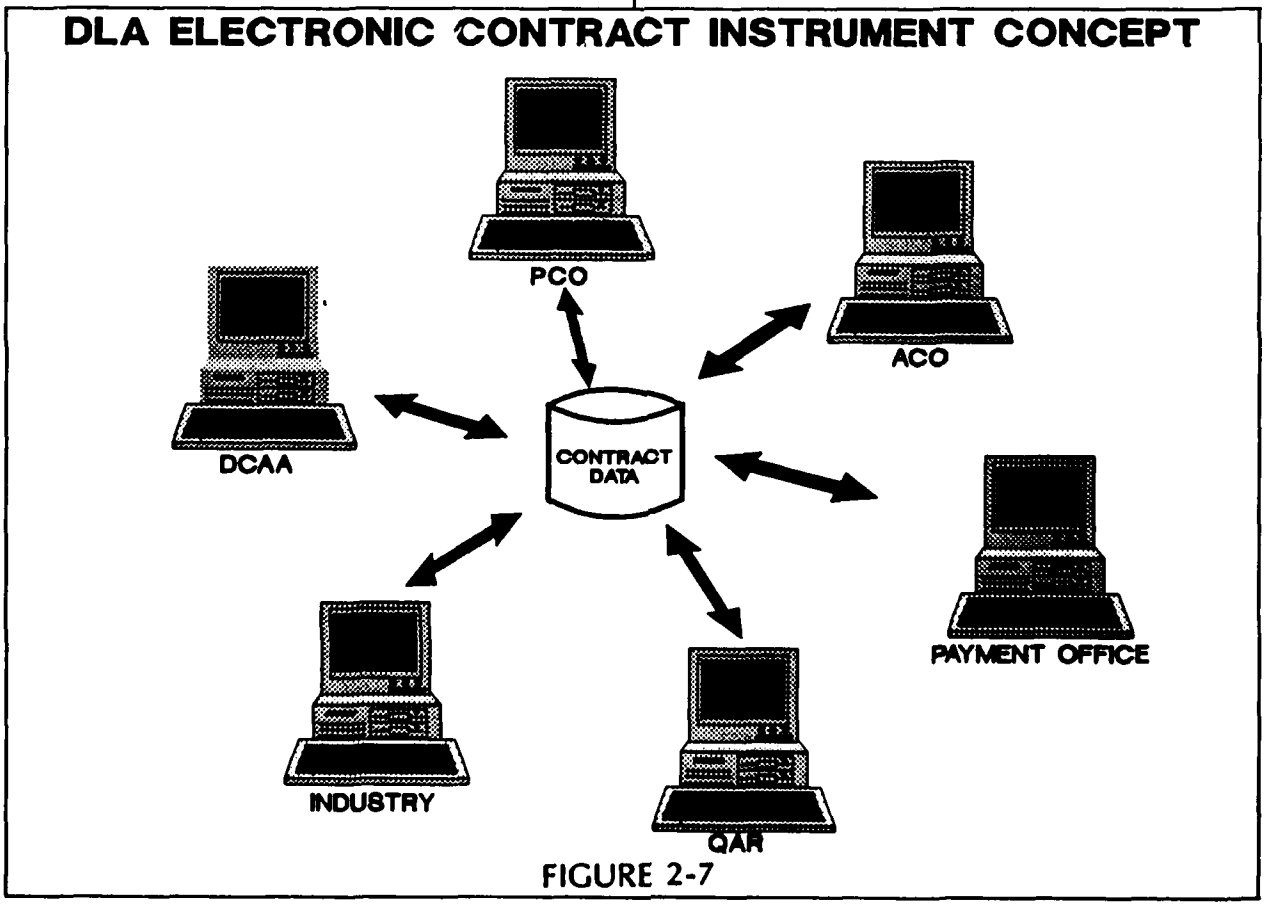


FIGURE 2-7

and determine the status of contracts awarded by DLA. The contract format will have uniform data elements that may be easily accessed by any cognizant activity regardless of the type of contract or source. Standardized data elements will allow users to access, with precision, all information required to effectively perform contract actions.

Throughout DLA and eventually DoD and Government agencies, every function will be able to input, access, and update information which they now provide manually. Provisions will be made to continue to handle contract data for those Government agencies that do not have the capability to access the database. Contractors will be required, when feasible, to input specific data, such as production and delivery status, price/cost information, and requests for contractual changes."

2.4.3.2 **Electronic Supplier/Customer Network (ESCN)**

"The purpose of ESCN is to connect the large, heterogeneous, geographically dispersed business community efficiently with the customer. It is a new approach to Government procurement by computer. ESCN speeds up the procurement process. In addition to current pre-arranged contractual agreements with a single vendor, ESCN allows rapid communication with multiple vendors. The ESCN concept should reduce the supplier's overhead cost of communicating to many small customers and will increase the current speed of transaction and material flow. It will speed up the transaction cycle: request for quotation (RFQ), quotation, order, and delivery. ESCN is particularly convenient for dealing with DLA's many small customers that mainly purchase in small quantities. DLA's Electronic Supplier/Customer Network will receive requisitions for items from customers, obtain offers from suppliers, evaluate them and place orders for items. Figure 2-8 portrays DLA's ESCN concept.

2.5 **Planning for Defense Logistics Modernization**

The DLA tasked the Board on Telecommunications and Computer Applications, Commission on Engineering and Technical Systems of the National Research Council (NRC) to review its modernization plans as they were evolving. The NRC team concluded that "doctrinal and policy issues, each of which influences the direction and scope of 'root' decisions at service and agency levels leave the logistics information systems communities groping for leadership and direction in many basic areas. The

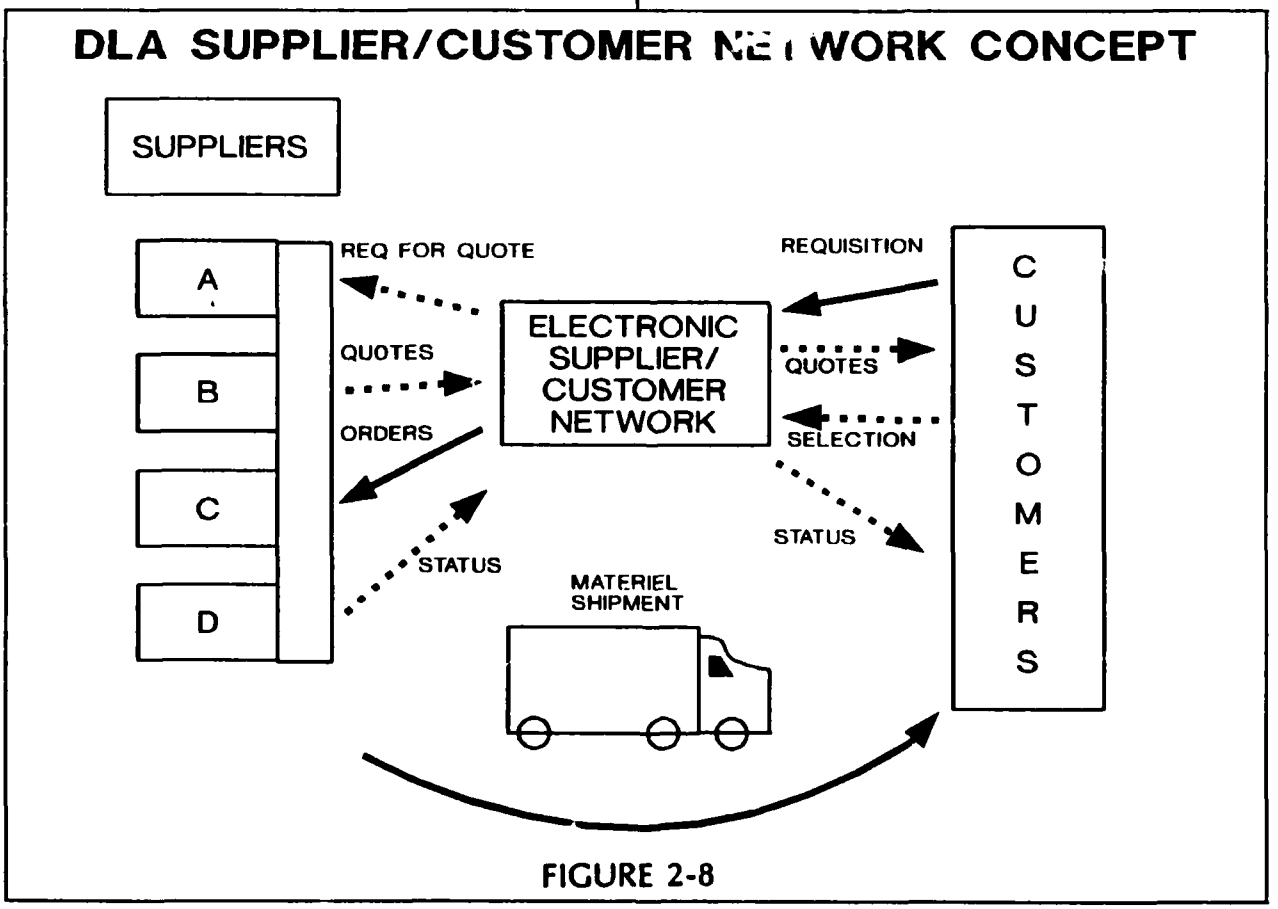


FIGURE 2-8

sufficiently important to warrant additional policy guidance directives by the OSD. [Only seven of the fifteen cited by the NRC are considered germane to the topic of this report.]

- Development of budgets and buy decisions using weapon systems application, essentiality, and programmatic data. Inherent in this guidance is the need for interchange of application, production, and deployment data across all DoD activities. This is needed to improve weapon system availability without increasing stock levels.
- The degree of customer access to asset and technical data held by the National Inventory Manager and central repositories. This would optimize decision making and improve readiness and efficiency. Such guidance is also needed to properly size ADP and telecommunications capacity.
- Contract administration structure and system design essential to maintaining an aggregate profile of contractor capability and performance. These profiles would permit more timely decisions in the buying process.
- Cost data elements, procurement history, and technical data that should be maintained and the degree to which such information should be accessible to buyers. This guidance would facilitate adequate system design and response to meet specified production and administrative lead-time goals.
- A forced discipline for electronically interchanging data between buying and contract administration offices. This will increase the accuracy of and concurrence of data passed between buying and contract administration offices.
- A framework for centralizing administration, accounting, and finance functions in an environment where ADP and telecommunications capability will make functional performance transparent to the physical location.
- Protocols, standards, and circumstances in which mandated data sharing and data interchange will reduce uneconomical duplication of data bases. This is needed for planning and specifying interoperable systems."[5]

The NRC team addressed other relevant issues which are excerpted in subsequent paragraphs.

2.5.1 **Data Bases**

"Throughout the briefings and particularly from examining the various BAA [Business Area Analysis] reports, we became convinced that the system modernization inherent in the LSMP [Logistics Systems Modernization Program] concept affords the DLA an unparalleled opportunity to create accessible data bases consisting of data elements needed to serve many different but related functions. We suggest that the DLA consider categorizing its data bases into three groups - technical, operational, and management. The *technical* data base includes: provisioning, cataloging, drawings and other technical type data included in bid sets, and the approved sources when applicable. The *operational* data base includes: inventory managers' demand history, assets on hand, under-contract quantities and on-order quantities not awarded, in-transit, applicable portions of contract files, and excess assets outside the normal reporting system. Data normally maintained for use by buyers in the procurement process are considered to be in the operational category. Customer orders in process at the inventory control points or storage depots are also included. The *management* data base includes those elements of data that account for budgets, fund expenditures, performance appraisals, and staffing.

In FY-87 the DLA supply centers bought and sold about $12.4 billion of fuels, subsistence, clothing, medical supplies, and hardware. Imbedded in the cost of these supplies are the capital expenditures made by defense suppliers for their own information-generating systems. Yet, there is no forum for coordinating government and industry information systems. To the extent that the defense supplier base is contractually supporting and servicing the agency's needs and generating the data necessary to fulfill contractual requirements, and to the extent that the agency itself is generating data for its needs, it would be in the interest of both to establish compatible electronic linkages that reduce the cost of both, and thus those of the DoD as a whole. Any long-range view of a modernized logistics management process for the DLA should encompass the desirability of such linkages."[5]

2.5.2 **Architecture and Standards**

"The current DLA system architecture is a hybrid configuration of multiple and autonomous computer facilities that cannot be interconnected and that cannot share data through electronic exchange. Further, since the applications do not work from a common or shared data base, on-line searches and exchange of data across centers are not possible.

While much of the literature on distributed data processing exaggerates the current capability of that technology, a great deal can, nonetheless, be accomplished in a well-designed system that has been built expressly for distributed processing. Additionally, the technology is improving rapidly. Within the time frames for the LSMP, we expect that a distributed processing system that is both robust and database driven will provide a cost effective capability when compared to the centralized architectural alternatives.

Considering the DLA's dispersed operations and the applicability of distributed processing, we recommend that the LSMP plan on capitalizing on this technology when it develops its technical architecture requirements.

Establishing information system standards early in the LSMP development cycle is vital to the successful integration of information within the agency and to sharing information across the service. Such standards also affect portability and the cost of software maintenance. Standards apply to the near-term improvement projects known as critical baseline enhancements (CBEs) and their transition to the LSMP architecture. The standards that should be established for the LSMP include those that deal with network communications, hardware architecture, operating systems, programming languages, and data bases.

The OSD has provided policy guidance (memorandum from Joseph Wright, June 22, 1987, on file; and memorandum from Donald Latham, July 2, 1987, on file) on the use of Open System Interconnection (OSI) standards (U.S. Government Open Systems Interconnection User's Committee, 1987), and the DLA should adopt these while posturing itself for new DoD initiatives such as the Computer-aided Acquisition and Logistics Support (CALS). Since OSI standards are not currently implemented in all vendor equipment, the DLA should incorporate *de facto* standards such as those employed for the Defense Data Network (e.g., TCP/IP protocol)."[5]

2.5.3 Security

"Security issues are a major consideration for the LSMP. Security refers to the protection of information from unauthorized ...[destruction, disclosure, modification, and denial of use]....Protection may be required while the information resides in computer systems and while it is being transmitted over communications systems. For information bearing national security classification, well-developed procedures exist for its storage and transmittal in hard-copy form. Trusted computer systems are in the process of being characterized and certified (U.S. Department of Defense, Computer Security Center, 1983). Trusted computer networks are more difficult to specify, but the effort is being made (U.S. National Computer Security Center, 1987). In general, stand-alone computer systems are much easier to keep secure than are interconnected ones. End-to-end telecommunications security is hard to achieve and rests mainly on the development of third-generation terminals capable of encrypting digital data.... Some unclassified but sensitive information requires protection for proprietary and procedural reasons. In response to this awareness, President Reagan, in 1984, issued National Security Decision Directive 145 (NSDD 145). Among other things, the directive established responsibilities for providing telecommunications- and automated-information systems security guidance to the departments and agencies of government. Measures for achieving such protection are not well standardized. Public Law 100-235 (U.S. Congress 1988) recognizes the problem for government agencies and gives responsibility to the National Bureau of Standards (NBS) in coordination with the National Security Agency (NSA) for developing computer security standards and training for the civilian federal computer systems and managers. The intent of the new law was to arrange that a nonmilitary agency, NBS, would relate to nonmilitary systems, while leaving a military agency, NSA, to relate to military systems. The new law does not change the relationship between the DoD, NSA, and the National Computer Security Center.....The available technology, as just noted, is limited in its effectiveness and can quickly accelerate a system's cost. Employing security measures without care for compatibility and transparency can restrict operations and severely limit hardware and software options. Sharing of data would be reduced and maintenance costs would be greatly increased. The use of security measures should be based on advice and assistance from the OSD and the NSA. In general, we suggest that security measures be evaluated based on the value of what is being protected, the severity of the threat against it, and, hence, the risks associated with its misuse. This will also require balancing of the cost of security at several levels of implementation against the probable consequences of compromise. We also expect that some operating efficiencies will be sacrificed because of restrictions in the distribution and common use of information. While it may be difficult to quantify this reduced level of integration, it should be included as one of the cost components of security. The DLA is investigating security requirements in the light of current policy. The agency should expedite this process and conduct a cost-

benefit analysis to determine the trade-offs and practicality of imposing security requirements. Since security will have such a major impact, it should be dealt with as soon as possible and not be deferred."[5]

1. Computer-aided Acquisition and Logistic Support (CALS), *Software Technology Service Bulletin, 16 December 1988, IDC Washington, Inc., Vienna, Virginia.*

2. CALS Briefing Will Feature Noted Speakers, *Government Computer News, 17 April 1989, Ziff-Davis Publishing Company, New York, New York*

3. First Public US ODA Demonstration a Success, *CALS Report, Vol. 2 No. 2, page 7, 2 February 1989, Knowledge Base International, Houston, Texas,*

4. 1988 Conceptual Functional Requirements, *May 1988, Defense Logistics Agency, Alexandria, Virginia.*

5. Planning for Defense Logistics Modernization, *1988, National Academy Press, Washington, D.C.*

3.0 AUTOMATED INFORMATION-

INCREASING THREATS TO SECURITY

This section addresses the security situation of current DoD component logistics-type systems. This situation will be untenable unless security is a mandatory design criteria in all CALS implementation initiatives. As previously noted, CALS Phase I is limited to unclassified processing. The term "logistics-type system" applies to all those employed in the research, design, acquisition, manufacture, provisioning, supply support, maintenance and training support of military platforms and weapons. This includes all the heretofore hardcopy documents these systems produce, directly or indirectly -- all of which are considered, with few exceptions, as unclassified systems.

The decade of the Eighties has seen no abatement in espionage and intelligence activities in the world. Several dozen U.S. military, Government and Government-contractor employees have been tried and convicted of providing Communist-block nations classified military information on a wide range of topics. A Government employee was convicted of providing unauthorized classified military data to a U.S. ally. There have been over a thousand *known* unauthorized disclosures of classified information since 1977.[1]

Commencing in 1984, the U.S. started reducing the number of its employees, and contractors, holding security clearances at any level. Foreign nationals in the employ of Government and Government contractors could no longer be granted clearances; U.S. citizenship became a prerequisite for Government and contractor personnel to receive a clearance. Non-citizens having a current clearance cannot now transfer it if they change employers. Companies lost their facility clearances, and their employees their clearances, when they no longer had active DoD contracts requiring clearances. The total number of cleared people (Government and contractor) dropped from 4.4 million in 1984 to 3.2 million in 1987.[1]

Attempts on the part of the Government to stop the outflow of high technology capabilities (e.g., supercomputers) and military technology (e.g., silent running propellers) from both the U.S. and its allies have persisted and been strengthened. Today the Government expends considerable resources to prevent the outflow of specific technologies and to monitor that of others.

And while all this was going on, NATO Governments, universities and contractors were busily building massive interconnected computer utilities with a view towards sharing information and each others' software technologies. The advent of these utilities has introduced new words into the ADP/T lexicon, such as virus, trapdoors, hackers, etc.

Through Logistics 2010, MODELS, CALS and the numerous implementing DoD component initiatives, the computer utilities of the military services, the defense agencies, defense contractors (here and abroad) are all in the process of being greatly expanded. While these expansions take many forms (e.g., greater automation, new types of automation), all focus on optimum connectivity and the maximizing of electronic data exchange and data sharing in lieu of traditional hardcopy communications. CALS is focusing on technical data (e.g., drawings, specifications, manuals) previously only promulgated in hard copy form at considerable expense and time delay, and encumbered with a prodigious logistics problem to maintain it current. MODELS is focusing on greater interconnectivity and standardization in Defense logistics systems, and electronic data interchanges with industry. And, Logistics 2010 encompasses both CALS and MODELS while adding greater interoperability between all DoD component systems, including between logistics and C^3 systems. All of these initiatives and the acquisition/development programs they have spawned have been made feasible by technological advances - in computers, computer software and telecommunications - which were unthinkable a decade ago in the Seventies.

3.1 Security in Current Systems

Except for those whole computer systems which are contained in a single vaulted computer room or secured building with no external data links, no current computer system employed in logistics-type processing can be considered secure. Earlier this year, it was disclosed that "...three West German computer....hackers helped the KGB gain access to computer data banks of the Pentagon, the nuclear arms laboratory at Los Alamos, N.M., and the National Aeronautics and Space Administration....The KGB are believed to have used computer passwords and other information obtained from the hackers to penetrate U.S. Defense Department Staff data bank OPTIMIS and U.S. military supply depot computers....the hacker tried to gain access to some 450 computers."[2] In "April 1988....U.S. computer security authorities revealed that West German hackers seeking information on spy satellites and nuclear weapons had [had!] penetrated more than 30 computers at American universities, military installations and laboratories."[2] Happenchance not se-

curity vigilance detected these penetrations. A frugal astronomer, unhappy with a 75 cent accounting discrepancy in his computer bill, initiated an audit that led to the disclosure of similar security lapses at DOE's Lawrence Livermore National Laboratory and, ultimately, to the arrest of the West German hackers.

"The President's Council on Integrity and Efficiency recently called on the National Institute of Standards and Technology to provide agencies with more security guidance....It reviewed operation systems and software security controls at computer centers in the Agriculture, Energy, Health and Human Services, Housing and Urban Development, Transportation and Treasury departments, the Veteran Administration, the Government Printing Office, NASA and the Office of Personnel Management....MVS is the predominant operating system for federal entitlement, payroll, financial management, accounting, grants and general administration programs. Of the systems audited, the report said six disburse about $273 billion annually and eight of the systems support financial systems that controlled $1.4 trillion in fiscal 1987. Using an agency's own terminals, the IG staff exploited internal security weaknesses by disabling security checking for file accesses and converting the terminals into the functional equivalents of a 'master operator's console'. The reviewers said they were able to gain unauthorized control over the system because of the poor administrative controls and lack of adequate security software....None of the centers used security software to guard sensitive system utility programs....".[3]

The Air Force and OSD recently defended the Air Force's supply systems security guidelines which did *not* require a user to log-off when finished with a computer terminal for extended intervals. Nor do its systems log-off inactive terminals, so the user (e.g., the supply clerk, another supply clerk, a passerby) need not repeat the log-on process to continue processing.[4]

Note that the examples above have been drawn from public media. Individual logistics data centers are not likely to voluntarily report their security foibles, so it is unknown how widespread or frequent penetrations (inadvertent, deliberate, or malicious) are occurring, or even if the typical logistics data center is aware of a penetration when one has occurred. How could they be if the penetrator just happened by a logged-on terminal/workstation which was unattended?

As discussed in DLAM 5200.1, ADP Security Manual, the degree of vulnerability or relative risk of a system depends largely on the type of operational services provided. Vulnerability of a system or operation increases as the operational services offered become more complex.

3.1.1 User Friendly Focus

Since the inception of on-line terminal devices in the early Sixties, the principal focus in systems design and development has been to extend the power of the computer and its systems of files and software to the user. From the early rigid procedural and query-only dialogues, we have advanced to virtually unconstrained interactivity being extended to the individual user through shell commands, systems programming facilities, structured query languages, etc. Throughout these many years of investment and development, every effort has been expended to make interactive systems as easy to use and as near instantaneous in responsiveness as possible. As workstations have been extended to lesser skilled office and blue collar workers, simplicity and ease of use have progressed even farther and response times must always be in the 2 to 5 second range, from across the base, from across the country.

The focus on ease of use and near immediate responsiveness has, in large measure, been achieved through computing and telecommunications power made available through technological advances and corollary advances in software capabilities. But, much of this achievement has also been predicated upon the suppression of prudent security features which were viewed as impediments to user friendliness, including responsiveness. User friendly has won over security in virtually every trade-off decision made on the part of the manufacturers, software vendors, data processing managers, designers and programmers. Whereas many of these same functionaries have argued against the "excessive" system resources consumed by software and database security mechanisms, few have similarly argued against the resources consumed to make their products user friendly. Besides, the system processes only unclassified inventory, accounting, procurement and/or contracting data, so why should anybody be concerned about security, many have asked.

This emphasis on user friendly goes far beyond ergonomics, and its mindset can create an insecure environment for CALS. Illegal access was gained to the Internet network last Fall by exploiting a bug in the Unix operating system. Computers that had not closed off all possible pathways between themselves and the network were most susceptible.

"While the invasion shocked computer users into realizing that no one's data is immune from attack, it

did not actually destroy information. Nevertheless, estimates for the cost of untangling the mess, plus the lost work time, range as high as $95 million."[5]

3.1.2 Unclassified Data Processing

The vast majority of logistics data (and particularly supply data - quantities in stock, requisitions, etc.) is indeed unclassified, as are the systems which process it. Further, in the absence of multilevel secure operating systems or instances where all users have the same level of clearance, unclassified data cannot be processed on the same systems with classified data. Hence, once segregated from the highly classified data and relegated to the unclassified masses of information, concern for security is relaxed.

Yet, is all this data truly that unclassified? A DD1348 requisition from a Navy unit having a priority of 01 through 03 represents that the requisitioner is "Not Mission Capable Supply (NMCS)"[6]; a situation requiring the unit to file a Casualty Report (CASREPT) with its commanders. Whether the priority is 1, 2, or 3 indicates the nature of its criticality to our offensive or defensive force posture. The MILSTRIP and NAVCOMPT Manuals to interpret the DD1348 and name of the requisitioner, respectively, are unclassified. The DD1348 is unclassified and is transmitted in the clear by radio, satellite and land line. The CASREPT is classified, encrypted for transmission and employed to update FORSTAT data bases in the Navy's various echelon C^3 systems. The fact of whether or not the Navy's supply system can fill the requisition, and approximately when if not immediately, is reported back to the requisitioner in the clear. Interesting dichotomy; the operators are trying to keep their problem a secret, while the clerks are acting as if nothing out of the ordinary had happened. It is unlikely that the doctrines and practices of the other military services are much different than the Navy's.

The example above is not unique to the Navy nor to requisitions. A good deal of the data processed by current systems pertaining to supply status, contract status and pipeline logistics can be exploited to reveal sensitive and even classified military situations. To date, logistics systems have been indirectly protected by two factors. The first is the volume of data and/or traffic which must be sifted through to discern important or relevant military force status information; NSA uses massive computers for this purpose to monitor the transmissions of other countries, are they the only ones using computers for this? The second factor is implicit in the fact that much of the current logistics data being bandied about so casually is in truth real data about supply activities, and only rarely contain the operating characteristics, material composition, dimensions, etc. of a platform, weapon, or avionics systems, or part thereto. But telecommunications traffic focussed on (or penetration of) the Defense Integrated Data System (DIDS) operated by the Defense Logistics Service Center could yield the thread to ultimately answer these questions for a persistent intelligence analyst/hacker.

The DIDS "system processes and maintains item descriptions for proprietary parts and drawings of supply items and weapon systems. The system performs cataloging transactions, produces supply publications and assigns stock numbers to all supply items in the system. The system also assigns commercial and government entity codes to contractors for purposes of cataloging and billing. Threats associated with systems relate to industrial espionage, spying, release of proprietary information to authorized persons....This [DIDS] system has not been officially accredited. A major modernization effort is currently underway which (by 1992) may result in all hardware and software being replaced. Accreditation will be completed as a part of the modernization effort."[7]

3.1.3 Distributed and Downloaded Data

During the Eighties, distributed data processing systems have become more prevalent even though the essential interface standards and system software products are only now reaching a degree of maturity. However, distributing data bases, a vogue but premature idea in the early Seventies, are far more complex to design, synchronize and sustain than they are to talk about. The result is usually a series of stepping stones or islands of automation, each operating under its own rules and administration. This physical separation provides a degree of security, until data files are exchanged between the islands or the islands are interconnected for interoperability. Unfortunately, data that is recognized as sensitive on one island (usually the primary source for maintenance) is frequently too casually treated on another island.

When the basic host operating system environments of interconnected islands are different, the disparity in the relative importance and/or sensitivity of the data is likely to be more pronounced. With the award of the AFCAC 251 contract to AT&T for 3B2 microcomputers, the 3B2 will in all probability become the standard departmental or middle tier/island processor for the next few years. Hence, the distributed architecture of systems and data will mostly commonly be IBM 3090 (or compatible)/MVS (XA)/DB2 (or ORACLE, etc.) at the

corporate tier, AT&T 3B2/UNIX/UNIFY at the departmental tier, and IBM PC-compatible/MS-DOS/ENABLE at the individual tier. Data integrity and security in this environment (which the Defense Logistics Agency has been attempting to implement for 3 years, but with Gould 9050s for hardware at the middle tier) is a challenging design problem and a complex operating environment. Once again, user friendliness and system responsiveness have been more important design objectives than data security - but the data is unclassified, just as the Navy Priority 2 requisition was above.

When the corporate and departmental tier computer systems are installed in one or more computer rooms (as is the case with the DLA's corporate processors and Goulds), there can be a modicum of physical and administrative security because they are in the hands of professionals. However, the size and characteristics of the 3B2 will permit its installation in any user office environment. Both its physical and administrative (systems administration, data administration, password administration, etc.) security will be more difficult to ensure. Sensitive data downloaded to them will be in much greater jeopardy of being compromised than were they managed, operated and administered by the data processing organization.

Data input, maintained or downloaded to intelligent workstations (e.g. Z248 Personal Computers) has no more protection than the facility provides the workstation itself. Yet, managers, professionals, engineers and clerks routinely leave restricted, sensitive and, probably, classified data in their PCs accessible to intruders and other unauthorized personnel. If the PC is hardwired (or with automatic dialing), and programmed for automatic log-on (including account code and/or password) as many are, to the departmental processor, and through it to the corporate processor, so much the easier for the intruder. Our inability, and almost timidity, to discipline or control the PC user environment creates a very weak link in the security chain. Not only is data input to them far too pervasive and too easily compromised, they, as workstations, jeopardize higher data forms downloaded to them, or make such data accessible to those without proper authorization.

Unfortunately, all distributed systems involve the use of computer terminals or workstations, their Achilles heel as regards security. These provide the doorways to the systems for all users, both good and bad. "If nothing else, the November attack [on Internet] has spotlighted the controversial role of hackers in modern society. In the computer community, the monicker means simply a gifted programmer, a wizard who can turn out elegant 'code' that other programmers admire, much as art aficionados appreciate a Picasso. At universities and research centers, adult hackers don't want to stymie the talents of the younger set, and some have even suggested creating safe havens, or computer dens where they can practice their craft without doing harm."[5] Since many universities and research centers are engaged in the research, development and support of military weapons systems, their faculty and graduate student workforces will also have a doorway to the CALS environment.

3.1.4 Drawings, Specifications and Manuals

Drawings and specifications contain data which is more important to unauthorized persons than other forms of logistics or technical data. They contain dimensions, material compositions, manufacturer's codes and part numbers, and assembly information, as well as references to other related drawings and specifications.

Today relatively few drawings and specifications, either classified or unclassified, are automated, but this situation is changing rapidly. As long as they were available only in hard copy, one usually had to gain access to the base, building, office and cabinet where they were stored in order to compromise them - no small feat for even the bravest of intruders. With the advent of computer-aided-design (CAD) in the Eighties, many drawings have been automated, but in islands of usually limited size. Those that weren't automated were probably committed to microfilm and, thereby, made virtually as safe or safer than the hardcopy, and for the same reasons. Few, if any, government CAD systems, such as the Navy's CAEDOS, were interconnected with other systems off base or shared with contractors. Their lack of inter-system interoperability made them as secure as are the PC workstations, but more so due to their complexity in operation.

Unclassified maintenance, operations and training manuals for military systems are very easy to obtain and can in some cases be bought from the government or on the open market. However, to be of optimum use, they must be current. This problem is probably as frustrating for spies as it is for the military. By the time most are available, the weapon or system they address has probably achieved its next level or two of modification.

Heretofore, physical acquisition of a hard document or microfilm was necessary to data collection of drawings, specifications, and manuals for illicit purposes. This is changing as we enter the Nineties. Their automation in a shared, interconnected, interoperable environment(s) employed by DoD and its

contractors, and our NATO allies and their contractors, is the ultimate objective of CALS.

Those few drawings and specifications which are now automated on hosts interconnected to a network or community of users are already vulnerable. It is not the automation of these drawings, etc. in CAD/CAE/CAM systems which in itself makes them vulnerable; it is the interconnecting of the host systems on which they reside to other hosts for the purpose of sharing their resources (which may not be intended to include the drawings) with other host-served communities of users.

The vulnerability was demonstrated by the 'wiley hacker' who penetrated MILNET. "Stoll [Clifford Stoll of Lawrence Berkley Laboratory] was able to piece together how the hacker entered U.S. computer systems. By making a local call in Hanover, the hacker reached a European data network known as DATEX.

From DATEX, he tapped into a library computer in West Germany's University of Bremen, and by manipulating software in that system was able to appear as if he were an authorized user with special privileges.

He then ordered the Bremen computer to telephone a U.S. computer network called TYMNET, which in turn connected the hacker to the Lawrence Berkley computer. The hacker, exploiting a hole in the software, was able to make himself appear as a legitimate Lawrence Berkley user, and with that identity had access to MILNET."[8]

This same incident also illustrated the security measures that had to be penetrated. It is conjectured that it required the 'wiley hacker' at least six months to penetrate the vast network of interconnected systems. This was because each system had to be penetrated separately before proceeding to the next system.

3.2 Vulnerabilities in CALS Standardization

The purpose of this section is not to wrestle with the vissitudes of carrying out "the largest standards effort in the history of computers,"[9] but to address how the standards adoption process and products resulting from these standards impact the security and integrity of government and industry CALS-compliant systems when implemented, in whole or in part. From the outset, it must be understood that the pervasive standards essential to CALS will, when implemented, virtually eliminate one of the inherent safeguards in existing and earlier systems, their very uniqueness from one ADP/T site or company to the next. This uniqueness has been a second line of defense which has been weakening for years as language and system standards have achieved greater acceptance. CALS will essentially eliminate it and rely upon access controls (the first line of defense).

Standardization of data format does increase the vulnerabilities of the CALS information since it simplifies the task of interpretation. This does not diminish the threat of unauthorized access to the information, but does suggest that the barriers of security are reduced with the uniform compilation of data and the commensurate distribution of this knowledge to a larger population of users, analysts, managers, etc.

The successful implementation of CALS initiative within the Department of Defense (DoD) and between DoD and the defense-aerospace industry is dependent upon the development, adoption and implementation of numerous standards. These standards must address a wide range of technologies and, therefore, become but one thrust or special interest focus among many competing interests. No longer is the federal government the dominant influence in the information processing industry that it was in the Fifties and Sixties. While it still represents a significant single marketplace for technology products, the sum of other marketplaces is now considerably larger. Nor does the government represent itself in a singular manner as regards product preferences and standards, since it customarily retains ADP/T systems long after they have become commercially obsolete. The adoption of standards essential to CALS must also be integrated with other related Government standards initiatives (e.g. GOSIP), and with those of other major market segments (e.g. EDI).

The populating of CALS-compliant systems throughout the DoD and throughout the defense-aerospace industry is an awesome undertaking which shall take years to come to fruition. To achieve its objectives, the CALS initiative will have to *sell* the commercial supplier and support service industries (singly and collectively) that it is in their best self-interests to become CALS capable. Further, this conversion to CALS will not permeate to DoD's thousands of small suppliers and service contractors until the essential products to augment their existing systems to make them CALS compliant are universally and economically available. It cannot be expected that such companies will all replace their whole ADP/T systems to become CALS compliant.

Given the increasingly international nature of the defense-aerospace industry, with increasing numbers of systems and parts coming from the Orient and NATO countries, and joint development programs

between the U.S. and other countries, the arena in which DoD-sponsored CALS standards must compete has become significantly broader in recent years. While there may be fewer suppliers to DoD in the domestic marketplace, those system, component and piece-part manufacturers outside the U.S. are also looking to other markets for their products which do not require CALS compliance.

3.2.1 Standards Adoption and Documentation

Standards for data exchange make all data vulnerability to disclosure to those without the need to know by the very process of their development and adoption. The adoption of ADP/T-related standards is a lengthy and very public process. All interested parties are engaged to varying degrees at various phases. The Government, standards and industry associations assume the mantle of representing the typical ADP/T user. Each representing their own, often parochial, views.

Subsequent to the adoption of a standard, and frequently before its final promulgation, companies having compliant products ready for the market include explanatory and self-promoting information in their sales literature, proposals and technical documentation. Some even go so far as to detail specifically what deficiencies the standard cures; and point out the deficiencies of those non-standard products on the market.

Once a standard is finally adopted, it is published in sufficient detail to enable manufacturers and suppliers to make their products specifically or functionally compliant with it. These standards can be purchased directly from the Government or from the sponsoring standards organization or association. Libraries can then be used to fill in the background information about how specific characteristics were derived.

In summary, to be effective, standards have to be both explicit and widely communicated. Those CALS standards already in existence, and those to come, provide current and would-be national and industrial spies a wealth of information about the inner workings of his or her potential victim's internal technical data processing environment.

3.2.2 Training

The vulnerability of systems employing standards is aggravated by the availability of technical training in the standards to large populations of users.

Technical training is available from many sources in many forms. Of particular interest to legitimate and unauthorized users, is that offered by the original manufacturers or producers of ADP/T products. Such training is usually offered at various skill levels from basic to expert.

Not only are each of the features, and the appropriate federal standard, covered in detail in formal training courses, so are all the "do's and don'ts" associated with use of the products; including those associated with overall systems or data base security. If that is not enough, the instructor always has a few horror stories to reinforce his or her point about the importance of one of the product's "features."

In-house training sessions in standards, conventions and techniques can also be of particular use to a party wanting to illicitly collect information because they are customarily more unguarded. From fellow users participating in such training, our would-be spy can gain both knowledge of, and access privileges necessary to, the sensitive information maintained by other groups in an organization. Since most of the technical, logistics and contract data CALS encompasses is unclassified, it is likely that all participants in such in-house training sessions will have their security defenses down.

What CALS and Federal Information Processing Standards (FIPS) documents do not reveal to the would-be spy can easily be acquired through unclassified formal and informal training programs, conferences and workshops.

3.2.3 Predictability Through Standards

How do published standards impact systems and information security? They establish for the inquisitive the rules of the game with which all players must abide. By knowing these rules, and the implementing options/features afforded by them, our would-be spy can predict the characteristics of the systems environment he or she is attempting to gain access to or extricate information from. A few training courses, copies of the standards, technical manuals addressing specific vendor products/services, a terminal/PC and a modem are all the tools needed to go into business; and all are readily available.

The CALS-specific standards do not themselves establish all the rules. FIPS standards, vendor system/software products and industry practices all combine together to define systems environments. But the CALS standards will enable identification of the data content, syntax and patterns so the penetrator can discern what type data he/she is looking at, how to interpret it, and how to follow it to that which is the specific target of a search. CALS standards provide the basis for how the data can be interpreted in either systems-speak or image-speak.

From these data, direct intelligence can be gained and it can be correlated with classified or unclassified data from other sources.

The total body of standards necessary to achieve the degree of data sharing and interoperability aspired to by CALS will go a long way towards making each computer environment and data base reaction to both legal and illegal queries predictable, in both form and content. It is through this predictability that a practiced, expert penetrator can readily interpret information hosted on any interconnected computer system in the world. Hence, that unattended, logged-on workstation on the receiving dock at Clark AFB in the Philippines isn't really as innocuous as it seems.

3.3 Threats Implicit in Technical Data Automation

Currently, little of the technical data addressed by CALS is automated, and only little of that is in shared or interconnected data bases. Though much of the logistics-related support (i.e. supply inventories) and administrative (i.e. contract clauses) is automated in one form or another, little of it is in shared data bases. Shared in the context that it is accessible for direct inclusion in the processing at a system/site other than on the host upon which it resides. Initial computerized processing was begun in the military in the Fifties. Since then, logistics-related data has grown at an overall compound rate in excess of ten percent per year, as have the uses/processes it serves. Technical data, on the other hand, has been automated primarily for the production of reproducible masters for printing-distribution purposes and in design engineering and analysis for computerized graphic systems.

CALS proposes to automate all the technical data for transmission to minimize the promulgation/distribution of printed materials. Further, CALS champions the automation of this technical data via shared data bases. Interconnecting systems with information dissemination being accomplished electronically/digitally within DoD, the Federal Government and, between the U.S. and its NATO/SEATO allies, and between Government and industry. The automation of these data will have a synergistic effect with the other logistics data already automated. This will likely cause yet further automation being required to effectively manage the totality of information available to engineers, project managers, inventory managers, contract administrators, operators, etc.

The motivations behind the CALS initiative are to make more effective and efficient the entire range of activities in the weapons systems life cycle, from design through disposal. If the initiative's operational goals can be achieved, the DLA and the military services will benefit. They will be able to reduce inventory levels and to place current information in the hands of designers, buyers, suppliers, maintainers and operators when needed, thereby making each category of user more productive. Such goals have been made plausible by technological advances of the past and will be made economically more feasible by further technological advances to come in the relatively near future. Hence, the attainability of the goals espoused by the CALS initiative is a function of standards, management and investment. However, automation of the scope and magnitude envisioned by CALS does not come without costs in addition to the investment monies required by all participants. CALS will automate technical data on virtually a world-wide basis in such a manner as is currently limited to very progressive sites or organizations. While much of this data is currently viewed as unclassified, the complete functionality envisioned will require its integration with sensitive, proprietary and classified logistics and technical data either within the "system" or by the user. The security of these data must be preserved in the national and corporate interests of all users.

3.3.1 New Types of Technical Data Automation

There are literally thousands of islands of automation in DoD and in the defense-aerospace industry at this time. Very few of these islands are interconnected to the extent envisioned in CALS, and even fewer share any degree of interoperability. That is because each island's automated capabilities have evolved over time in response to its users' parochial interests and ability to economically justify each evolutionary step. Hence, technical data of priority interest to one island may have been originated by another where it was viewed with indifference as an organizational by-product and was, therefore, not suitably automated, if at all. This was and is particularly true of islands in different mission areas. For example, the users and systems of the Defense Electronics Supply Center and the Navy Aviation Supply Office, which are responsible for the piece part supply support of the Sidewinder air-to-air missile, do not have access to, or share data with, the systems of the Nielson Laboratory at Naval Weapons Center, China Lake where the missile was designed. Nor did NWC specifically automate the kind of technical data of direct interest to DESC and ASO. CALS will change this in the future.

By defining the standards and tools needed to automate and exchange all forms of technical data, CALS will slowly bring about the stratification and identification of all components of the data. This in

turn will nurture and expand the expectations of all users of technical data to ask for it more frequently in an automated form. Users will demand automated formats from their organization's systems and the systems of those organizations with which they deal on a day-to-day or even casual basis. Hence, not only does CALS promote greater technical data-document automation for individual users and organizations, it also stimulates the demand for the automation of such data from other users and organizations.

Inherent in this discussion is the large impact on security. The threat here is that new additions, changes, and deletions may lead to security cracks that were not considered in the design of the original system. Hence, maintenance of the system security will have to play an integral part throughout the life-cycle of all systems hosting CALS format data.

Many automation initiatives which were conceived before the advent of CALS (e.g. the Navy's Print On Demand System (NPODS)) to counter operational and/or cost deficiencies have come under the CALS umbrella because they aspired to redress many of the same problems as CALS. These initiatives, either local or service-wide, have addressed the automation of virtually all forms of technical and logistics data. Within the context and standards of CALS, local experiments with specific types of data can and will ultimately become global forms of automation.

Most categories of unclassified technical or logistics data are within the CALS concept of the future. It is easy to conceive how each may be automated and to savor the benefits which would accrue to both users and budgeteers from such automation. Even with current 1989 technology, virtually any type/form of data can be automated. CALS has made it both more saleable and justifiable. The evolving CALS standards have made it more feasible. Of particular importance is that these data will contain unclassified information that previously was only available in hard copy; such data as the frequency and power settings of an electronic jammer, the assembly and parts breakout of the jammer, the test points and thresholds of the jammer, etc.

The controlled, experimental automation of a sample of drawings, manuals, etc., in an organization's files/library may have minimal security implications. The automation of the entire collection presents a security issue of a different and greater magnitude. It is relatively easy to scan for a sample and suppress the sensitive information; scanning a collection is not as easily performed. Further, such automation transfers custodial control of a form of the data from the engineer, logistician or librarian and vests it in a system of hardware, software, operators and users.

Once a collection is automated, it must be maintained. Hence, the procedural operations of entire organizations must be modified. The automated collection also becomes the focus of a wide range of new uses. Whereas physical considerations previously frustrated manipulation of the collection, the only impediment becomes the automated user's creativity in conceiving search, selection and cross-correlation criteria. As we have seen with logistics data since the Fifties, this creativity is limitless, and not restricted to ADP/T technical personnel.

The automation of each category of technical data, or type of document/publication, may be viewed parochially as regards technical and economic viability, but it must be viewed from both local and global perspectives as regards security. If everything everywhere is automated, the protection of local data must be accorded on the basis of its contribution to, or filling out of, the total population of data available.

3.3.2 Data Correlation and Corroboration

The greater the breadth of the automation of technical and logistics data pertaining to a weapons system, the greater the opportunities provided an intelligence analyst or spy to compare data from one source with that from another source. This is an aspect of both international and industrial espionage, since it precludes erroneous analytical conclusions predicated upon deliberately leaked misinformation. With virtually everything automated in a multiplicity of systems, and also distributed in hardcopy (e.g. Request for Proposals, standards, manuals), such analysts can cross-correlate and validate their findings with relative ease, if they can gain access to the automated systems.

In the same manner, intelligence analysts can cross-correlate what they possess, or is accessible, to determine what pieces of information they are missing. Just as with footnotes and bibliographies in hardcopy documents, automated systems provide references, pointers and/or search arguments to information and expositions resident in other automated systems, and to hardcopy technical reference materials. Not only do these references point the way to corroborating information, they can also reveal sources of data previously unknown to the would-be spy.

With all this well-intended help for legitimate users, the spy doesn't have to climb over a fence to corroborate his findings. He or she need only gain access to one or more interconnected systems of computers and follow the trail of bread crumbs from

one system to another. "Once inside the systems, the hacker seemed to know exactly what he wanted; he would search for keywords like 'KH-11,' 'NORAD,' 'nuclear' and 'SDI.'"[8]

Extensive automation of technical-logistics data and reliance upon user accessible systems readily facilitates the cross-correlation, corroboration and collection of data. They also enable the aggregation of a sufficiently wide array of "unclassified" data from standardized system environments which, when taken all together, reveal facts or situations which are treated in command centers as "CLASSIFIED," or at least are sensitive Government or corporate information.

3.3.3 Global Technical Data Aggregations

During Phase 1 of the CALS initiative, the focus is to be limited to "unclassified" technical data. To gain added productivity and consistency, additional data must also be automated. The more data available in the system, the more attractive it becomes as a target. The value of information becomes more valuable as its depth and breadth increases. Thus, more should be spent to protect it. "This technical data includes part descriptions, product specifications, and standards that the initial designer draws upon; the engineering drawings and product data used in design and manufacturing; the information needed to guide the people who operate the system in the field, or who support and maintain it at all echelons of the logistic support structure; the materials needed to train new operators, maintainers and other technicians; and the information needed for reprocurement, remanufacturing, modification, and feedback to industry for future design."[10] This definition encompasses an enormous range and bulk of information, whether in digital or hard copy form. Further, a weapon system is composed of thousands of subsystems, assemblies, subassemblies and piece parts, and undergoes thousands of design modifications during its 10 to 50 year life cycle. Heretofore, most weapon system programs have been initiated with significant portions of their initial designs, characteristics or components being classified; some components remain classified throughout their life cycles.

It is likely that, if anything, our enemies have been, like ourselves, overwhelmed by the amount and varieties of information available during the life cycle of one of our weapon systems. If one were to collect copies of all the technical data, as defined above, about the Navy A-6 which went into service in the early Sixties, it is unlikely that it would fit into even a large warehouse. (A single bidder for the C-5A transport aircraft contract submitted 1,466,346 pages weighing 24,927 pounds"[11]; undoubtedly a small file when compared to the thousands of design, specification and engineering changes submitted since award of this multi-billion dollar contract.) Certainly any spy who attempted to accumulate that much data would have been caught upon leaving Grumman on his or her forklift, or one of the many Navy and contractor activities engaged in A-6 acquisition, support program, or operations. It can be concluded that the physical bulk of hard copy and the physical dispersal of portions of technical data to tens or hundreds of locations was in itself a passive security mechanism which precluded complete data capture. Hence, the spy assigned to collect A-6 characteristics and capabilities information had to be very selective in order to be discrete. It is likely that his or her targeted documents were design specifications and drawings as having the most telling information with the least amount of bulk. What those documents didn't directly reveal was available from other documents which they referenced (identified).

CALS proposes to automate all these documents, both the spy's original targets and *all* other technical data related to the weapon system. "The longer term goal of CALS is integration of industry and DoD data bases to share common data in an Integrated Weapon System Data Base (IWSDB) structure that is implemented through Contractor Integration Technical Information Systems (CITIS) and Government technical information systems....The technology to accomplish this will be incrementally implemented as it is developed and proven....The Government must identify during acquisition planning the provisions that should be developed for effective management of classified, sensitive, or limited rights data....Contractors should work with acquisition managers and contract administration activities to implement on-line access to data files, and to establish guidelines defining the actions on the part of the contractor and Government that constitute delivery and acceptance of data which may remain resident at the contractor's facility....Contractors must develop and follow procedures which ensure digital data delivered to, or accessed by, the Government are properly marked and that controls and safeguards in the digital environment provide at least the level of protection provided in the paper-based environment."[10]

In short, all technical data pertaining to "the Air Force advanced tactical fighter, the Navy A-12 advanced tactical fighter, the Army LHX light helicopter, and the Navy V-22 Osprey tilt-rotor aircraft"[12] are to be automated and protected by means com-

parable to those employed to protect the technical data of predecessor weapon systems.

We have postulated that logistics-type technical data can be employed to reveal classified, operational circumstances. Given the vast array of "unclassified" technical data to be automated, there are all too many permutations of data combinations that might compromise a weapon system's design, operational characteristics, technological innovations, etc. The replacing of hundreds of physical and/or incompatible, automated repositories of technical data with an interconnected, interoperable system of systems constitutes a massive aggregation of "unclassified" data. This aggregation has the potential to reveal virtually everything anybody need know about a weapon system, including what serial number and modification level is installed in what platform. "Although the bulk of this data will usually be unclassified, the inferences which can be drawn from the accumulation of unclassified data (data aggregation) may dictate a higher level of classification for the data elements or the aggregate data"[10] - such determinations are both hard to make and hard to implement without serious impact upon the utility of the aggregation. The purpose behind the creation of this automated aggregation "is to improve industry and DoD productivity and quality."[10] Unfortunately, if the aggregation can be penetrated, it can also yield the same benefits for those in international and industrial espionage.

3.4 Universal Technical Data On-Line - A Real Threat

There are currently, and has been for some time, various forms of unclassified weapon system technical data, as defined by CALS, accessible via on-line interactive systems. But, relatively little of this data has been hosted on, or interconnected with, systems accessible to the public. Further, there are probably fewer situations where these data that are automated are accessible via dialed interfaces or transmitted via satellite links.

Two issues must be addressed. The first issue is the magnitude of the increased technical data to be automated so as to be accessible on-line. The second issue is the proposed sharing of the data between Government, allies, industry and those commercial enterprises participating directly in the same weapon system life cycle program or through components common to multiple weapons systems. The advent of such an information environment as proposed by CALS will be accompanied by an exponential explosion in the population of users requiring access to the automated technical data, and a comparable increase in the volume of technical data being transmitted via public and Government networks. Further, increases in the host telecommunications facilities will be necessary to service the expanded number of users and higher traffic volumes. Like security in other environments, the strength of a security envelope is only as robust as it's weakest point. Hence, where one community/island of users practice and endure appropriate security measures, if it is interconnected to another having lower standards or interests in security, the latter establishes the strength of the ring for the former and the universe of users. System security administrators are faced with a challenge of immense magnitude and complexity. At issue or risk are not only national security interests, but also corporate proprietary data rights and the privacy of internal, sensitive Government and corporate business affairs.

A few of the concerns facing system security officers who must set standards for those over whom they have but nebulous control, are addressed in the following paragraphs. None of these concerns are unique to CALS, they just take on added dimensions due to the magnitude of the CALS initiative. Technical data system designers and operators must "...recognize that evolving technology and standards for system and data protection are being matched by evolving technology for protection infringement."[10]

3.4.1 System versus Facility Penetration

The international, political or industrial spy need no longer physically gain access to premises containing the sensitive information being sought. The penetration of, and/or the removal of hardcopy information from, a facility without detection and/or identification remains a high risk venture. Yet, the same result can be achieved with relative ease and in less time if the data is automated in a telecommunications-capable computer environment as required by CALS. Conceivably, a penetrator/hacker could be in and out of the system in less time than it would take to transit from an unlocked front door to an open second floor office, one way! Nor need a well-equipped and experienced spy even gain access to the systems, if he has appropriate passive monitoring equipment and can gain access to circuits connected to the system from any nearby(?) location. If so, all data being transmitted to or from the system can be screened for interest or intelligence. It is said that all satellite transmissions by both the United States and the USSR are monitored by the other. It is suspected that the Soviet Embassy in Washington, D.C. is capable of monitoring a significant percentage of the telephone conversations in the city and its surroundings.

As we have seen from earlier examples cited in this report and in the media, gaining unauthorized access to computer systems is not as difficult as we would like to think it is or should be. Much has been said and written over the years about the vulnerability of account code-password access protection features, direct-in or call-back dialed interfaces, data encryption, weak system security administration, etc. Still, remote system access capabilities present significant security and system integrity threats for classified, sensitive and unclassified Government and industry processing systems. The CALS initiative's goal of a global, interoperable, shared, automated technical data environment in support of each new weapon system life cycle poses risks of paramount importance to Government and industry. Solutions to these risks are critical to the success of the initiative.

3.4.2 Interconnected System Services

Last Fall, we read about the computer virus originated by a graduate student at Cornell which disrupted Government, industry and university systems around the country and the case of the West German hacker previously cited herein. Interconnected computer systems pose a range of security problems beyond those of a single system. The site with no dial-in ports, no off-base circuits and no gateways to other public or private networks has fewer, but no less critical, security and integrity problems. But, such systems are incompatible with the goals, objectives and characteristics of Government and DoD initiatives such as CALS. Figures 3-1 and 3-2 portray the interconnected system environment to be achieved by Defense Data Network (DDN) users and industry via electronic (business) data interchange (EDI) through Modernization of Defense Logistics Standard Systems (MODELS) initiative. Weapon system technical data is but one of many types of data traffic which shall be serviced by this architecture. Traffic in the network itself will be relatively secure assuming fiber optic and/or encrypted trunk circuits. However, the possibility that a user in one system can take on privileges so as to represent him/herself as an authorized user to yet other systems does exist as demonstrated by the West German hacker. Data can be illicitly extracted, programs modified (as the Cornell student did through an Email interface) and data modified, or worse. Once again, that logged-on, unattended workstation at Clark AFB does not seem as innocuous as it would appear.

MODELS FUNCTIONAL INTERFACES[13]

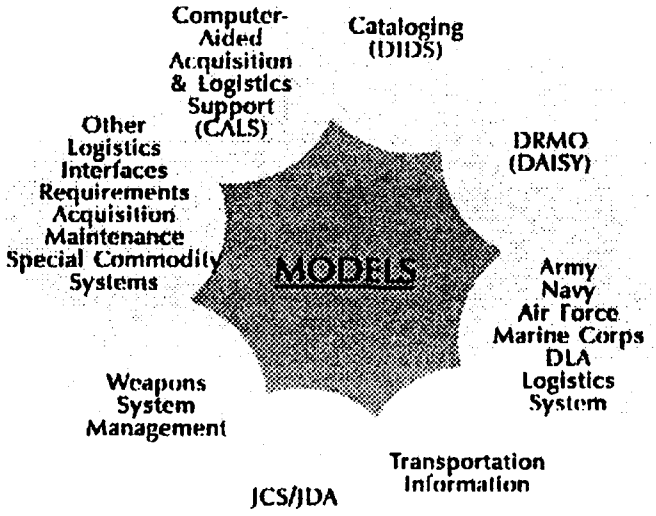


FIGURE 3-1

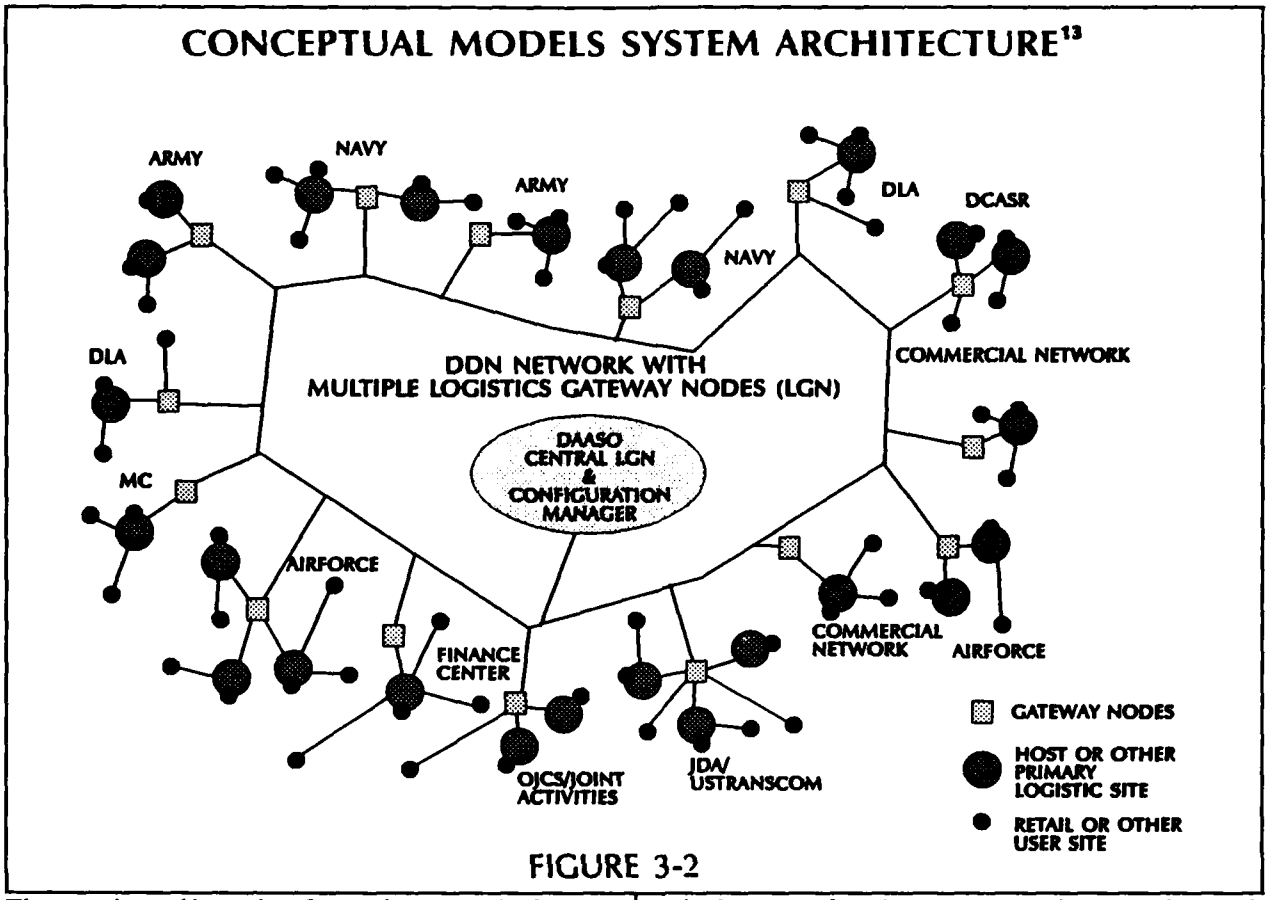


FIGURE 3-2

The security and integrity of an entire network of networks or computers is no stronger than the weakest link. Security administration in such a network or environment is only as good as that practiced by the least experienced, most indifferent or user-intimidated system security administrator in the network. It is through such a chink in the armor that a penetrator can assume unwarranted privileges that open the doors to other systems in the network of systems. Whereas, the National Computer Security Center can certify the component operating systems and data base management systems employed within a network of systems, no organization is charged with the *on-going* testing of this network to ensure that all systems in it are being properly administered. "The rapid expansion of networks presents another security problem, Hempel [Victor Hempel, Senior Technical Advisor to the Office of the Secretary of Defense] said, while networks 'make it easier for managers to access and process information, they also make it easier for our adversaries to get to the data quicker and faster'."[14]

3.4.3. Ease of Use Versus Security

The productivity benefits of on-line systems is falsely measured in terms of how easy it is to use; falsely, in that ease of use has no connotation as to the worth of such use. Almost any attempt by a system security or data base administrator to tighten security generates complaints from users claiming impediments to, or encumbrances upon, their productivity. Whether the individual user is a clerk-typist doing report preparation or an operations research analyst doing logistics support analyses is rarely a discriminator. Yet, the two obviously have differing system/data access needs and the worth of their contributions to a weapon system life cycle cannot and should not be viewed as equal. An axiom of security is "need to know", but "user friendly" and "ease of use" have become the operative axioms in unclassified data system operations.

Not only are individual system security and data base administrators being subjected to abuse by their user communities, the industry at large is developing and promoting concepts and tools (products) wetting the appetites of those same users by making computers easier to use as part of the "Information Age." No longer is a user, especially in the proposed CALS technical data environment, viewed as one constrained or limited to his or her organization's host system, but, rather, as someone having a potential

need to access any piece of information anywhere. Figure 3-3 exemplifies this new concept of user.

The advent of query-natural language interfaces to support interactive, ad hoc extraction of information from data bases is yet another manifestation of making computers easy to use or user friendly. Whereas, structured query languages (SQL) began as a programmer productivity-enhancement technique, it quickly became an expedient tool for those users who couldn't really define or anticipate their data needs during the design and specification of their employer's automated information system. Yet, if a weapon system program office cannot define specifically what combination of unclassified data might infer classified information, how can data base and system security administrators constrain the potential utility of their systems to illicit users when confronted with tools having the power of on-line SQL? Short of classifying each individual data element to each individual class (and pedigree) of user, they cannot without seriously impairing the system's "user friendliness".

The illicit retrieval of technical data is not the only thing system security and data base administrators should worry about. Of greater concern is the undetected modification of technical data files made accessible for the sake of being "user friendly." Who can foretell either the timing or gravity of an undetected change in the material composition, physical tolerances, or dimensions of procurement specifications for a single part to a weapon system? Who can foretell the impact of the stocks of the entire military supply system (wholesale and retail) being polluted by the re-supply of a part to a weapon system(s) which will not fit, will fail or bind under stress, will burn when it shouldn't, etc.? Who can foretell the impact of a "trap door" or "Trojan horse" which causes a military or industrial logistics system to fail under stress (e.g., mobilization workloads) or upon command.

Are not DoD logistics systems equally as vulnerable to illicit changes (or sabotage) in either data content or operating software? Is it not ironic that the CALS initiative comes to the fore when the industry as a whole is just now realizing the vulnerability of its systems?[16]

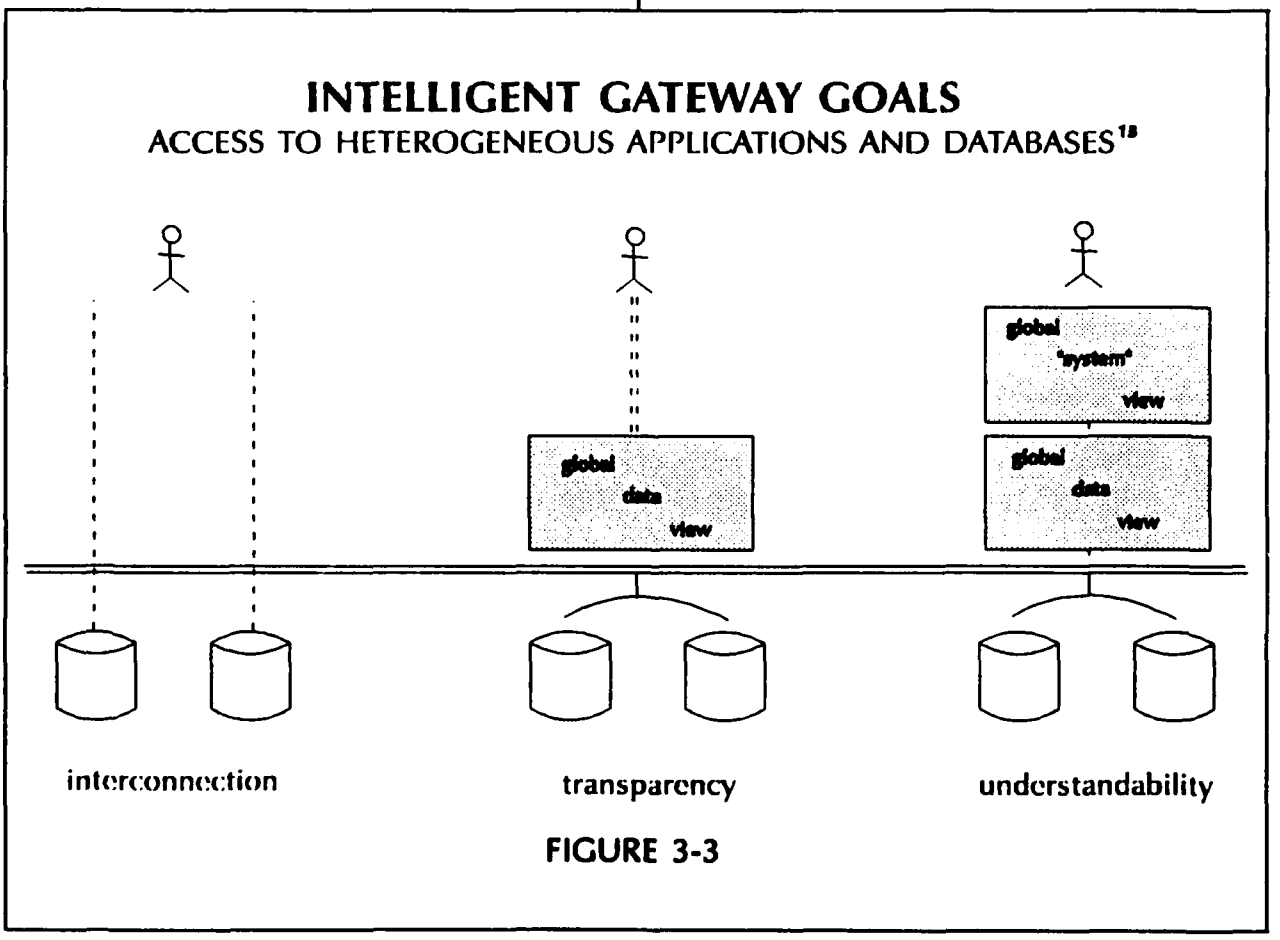


FIGURE 3-3

1. Information Security, Update of Data on Employees Affected by Federal Security Programs, *GAO/NSIAD-89-56FS, 7 March 1989, U.S. General Accounting Office, Washington, D.C.*

2. German Computer Hackers Held for Spying for Soviets, *March 3, 1989, The Washington Post, Washington, D.C. [can be electronically retrieved on NEXIS through Mead Data Central].*

3. Security Guidance is Urged for Govt. Computer Centers, *February 6, 1989, Government Computer News, Ziff-Davis Publishing Company, New York, New York.*

4. Supply Security, Air Force Controls Need to Be Strengthened, *B-230505, 12 February 1989, GAO/NSIAD-89-34, U.S. General Accounting Office, Washington, D.C.*

5. Viruses Pull Computer Underground Into Spotlight, *5 February 1989, The Washington Post, Washington, D.C.*

6. Military Standard Requisitioning and Issue Procedures, (MILSTRIP) *DoD 4000.25-I-M, May 1987, Department of Defense, Washington, D.C.*

7. Defense Logistics Agency Security Plan, *10 January 1989, Defense Logistics Agency, Alexandria, Virginia [For Official Use Only].*

8. Computer Detective Followed Trail to Hacker Spy Suspect, *6 March 1989, The Washington Post, Washington, D.C.*

9. User's Needs Drive CALS Effort, *Government Computer News, 15 May, 1989, Ziff-Davis Publishing Company, New York, New York*

10. Department of Defense Computer-aided Acquisition and Logistics Support (CALS) Program Implementation Guide, *MIL-HDBK-59, 20 December 1988, Washington, D.C. 20301*

11. The Paradoxical Proliferation of Paper, *March-April 1988, Harvard Magazine, Harvard University Alumni Association, Harvard, Mass*

12. CALS Briefing will Feature Noted Speakers, *Government Computer News, 17 April 1989, Ziff-Davis Publishing Company, New York, New York*

13. *From the Defense Logistics Standard Systems Office Presentation at* Electronics Data Interchange: Bringing It Together in Government *Conference, May 26, 1988, National Bureau of Standards, Gaithersburg, Maryland.*

14. OSD Expert Says Government Should Inspect Source Code, *Government Computer News, 6 March 1989, Ziff-Davis Publishing Company, New York, New York.*

15. Object-Oriented Intelligent Gateways *Sandy Heiler (Computer Corporation of America), 29 September, 1987, CALS Intelligent Gateway Conference, Planning Research Corporation, McLean, Virginia.*

16. Computer-Protection Market Grows, Thrives on Fear: Many Virus Remedies Are Only Placebos, *23 May 1989, The Washington Post, Washington, D.C.*

4.0 SECURITY PERFORMANCE MEASURES

This section discusses the measurement of security performance. The impact on CALS is noteworthy. Security performance measures for classified systems are well documented. However, little guidance is available for managers of unclassified, yet sensitive or proprietary, systems and data bases.

Depending upon the eyes of the beholder, system security can be measured in either binary expression (is/is not) or in relative terms. Systems processing classified data must of course be measured on the binary scale. Systems processing unclassified data are more apt to be adjudged in relative terms. Ease of access versus authorized need to know is the balance point system security managers seek, so there are trade-offs to be made between the interests of the users and the *interests of the users*. Their interests in terms of the relative ease of their authorized access and data use, and their interests in terms of confidence in the integrity of the data provided them and in the appropriate safeguarding of their data. In this sense, security to the user is as binary as though the data were classified. Yet, most communities of users, and their security system administrators, over time tend to err by tipping the balance too far towards ease of access/use. System security or integrity in unclassified data processing systems is achieved through a combination of components, just as in those processing classified data. Figure 4-1 illustrates the principal components and their interaction.[1] Note that a breakdown or weakness in any component compromises the integrity of the whole. In other words, the weakest link determines the security of the total system.

Though this illustration was drawn from a publication of an organization promoting security of classified data and computer systems, the principles are equally applicable to all other systems. The U.S. intelligence community has concluded "that Soviet intelligence collection activities have been aided by on-line access to commercial electronic data bases, which, though unclassified, contain Department of Defense and Government-funded contractor studies dealing with the design, evaluation, and testing of U.S. aerospace and weapon systems...[and]...that in recent years the growing use of electronic data bases accessible by remote terminals has provided the Soviets with an efficient means of identifying and

LINKS IN THE CHAIN OF COMPUTER SECURITY[1]

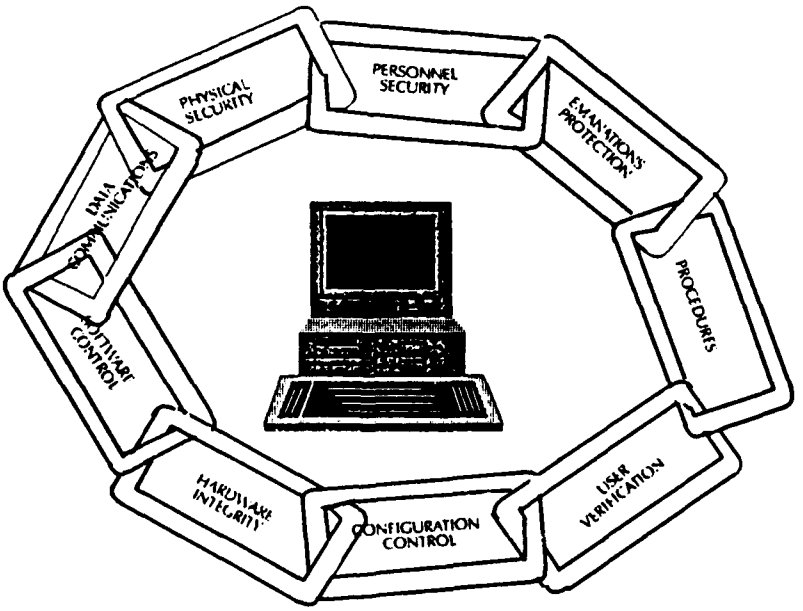


FIGURE 4-1

procuring unclassified technical information needed by Soviet weapon designers."[1]

4.1 Internal versus External Threats

Not all threats to the security and integrity of a system come from outside the organization. An equal number come from within, but the most notable is the all too common mindset that security is not important, too hard (i.e., not user friendly) or not worth the time and money--this is irresponsible, unprofessional malfeasance regardless of the purpose for which the system is operated. The following provides a representative tabulation of internal versus external threats to an unclassified data processing system, or network of systems:[2]

Internal threats (within the institution)

Employees:

- Greed, malice, ineptitude, accidents, disgruntlement.
- Bogus transactions
- Trojan horse (unauthorized procedures hidden within programs)
- Unauthorized copying of data
- Modification of data
- Unauthorized sale of data
- Destruction

System Failure:

- Failure of computer programs
- Loss of data from system malfunction
- Failure of hardware components
- Deterioration of storage media
- Failure of communication links or programs
- Failure of power

External threats

Human:

- Criminals, terrorists
- Physical damage
- Destruction of data
- Modification of data
- Theft of data
- Fake transactions
- Impersonation of authorized user
- Forged access devices
- Unauthorized use of access devices

Natural disaster (fire, flood, ice and snow, earthquake, etc.):

- Direct damage
- Lack of maintenance
- Overload at terminals
- Inaccessibility

Data protection and integrity requirements for CALS are divided into six interrelated security disciplines: communications security, computer security, operations security, physical security, personnel security, and information security. These disciplines must be integrated into an overall systems approach."[3] Of particular importance in CALS is that it encompasses on-line data sharing amongst whole communities of Government, academic and contractor entities participating in a weapons system program, including many with only a passing interest in system security and/or integrity. Whereas "Government technical information system managers must share with CITIS [Contractor Integrated Technical Information Systems] managers responsibility for protection of classified, proprietary, or otherwise sensitive information....small businesses should not be put at a disadvantage because of limited resources for the investments needed to comply with CALS data delivery, data access, and functional integration requirements."[3] Hence, each participant in a weapons system program must, directly or indirectly (but still at the ultimate expense of the Government), implement a system security program which addresses all possible internal and external threats to its integrity. The implementation of the program should be "on the basis of formal risk versus vulnerability assessment procedures"[4] in order to avoid becoming the weak link in the chain. DoD Directive 5200.28 provides guidance for mandatory minimum AIS security requirements. More stringent requirements may be necessary for selected systems based on acceptable levels of risk.

4.2 Physical versus Logical Security

The physical security of a computer system primarily addresses access to the computer equipment itself. It is reasonably feasible if the computer is contained in a single enclosure (e.g., room, building) and has no external devices (workstations) outside the enclosure. It is less feasible if the system has workstations scattered around the base/compound. It is infeasible in networks of computers as currently exist

and as proposed by CALS. In the latter two cases, physical security must be buttressed with 'logical security'. That is, "access controls must be electronically coded into the logic of the computer's programming. This is usually accomplished with password systems, although there are other methods [not identified] as well. A password system will not foil an expert technician with access to the 'guts' of the machine, and it will not prevent physical removal of data stored on disks and tapes."[1]

Research and development is rapidly progressing in the development of "logical security" mechanisms, some of which involve physical devices (data encryption chips). But, performance measures have not been developed for the application of those that have been developed. The Commercial Product Evaluation Program of the National Computer Security Center does evaluate and assign a rating to logical security products (e.g., computer operating systems)[5]. But there is no organization or system of follow-ups to assure the weapon system program office security officer or technical information system manager that program participants are effectively employing them in their stewardship of unclassified technical data. Large prime contractors having adequate managerial, technical, and security staff resources can be obligated to adhere to certain contractual standards of performance, and perhaps can be relied upon to comply with them, but what of the second and third tier contractors? Is it enough to say, "the acquisition manager and potential prime contracts should jointly pay particular attention to data requirements that will flow down to subcontractors and suppliers."?[3] Can we assume that these subcontractors and suppliers, singularly or collectively, do not present the potential of being the proverbial "weakest link in the chain"?

Every commercial participant in a CALS-compliant program can potentially benefit from applying published Government standards in their everyday data processing activities. "In the private sector, we know that computer crime for the purpose of fraud and embezzlement is extensive - much of it undetected or unreported. According to one estimate, $300 million is lost each year to computer criminals. We also know that the gaps in security that permit computer crime, fraud, and abuse in business and Government are the same conditions that would make classified and sensitive defense information vulnerable to collection by hostile intelligence agents"[1] and industrial spies. The following categorical listing of Government standards and guidance for security in unclassified data processing operations are applicable to every participant in a CALS-compliant weapons system acquisition program, even though none provide specific quantitative or scales of security performance measures (a full title and abstract of each is included in Appendix A.[6] Additionally, Appendix D provides a summary listing of directives, regulations, and guidance documents dealing with computer security).

Contingency Planning

FIPS PUB 87

SPEC PUB 500-85

Database Security

FIPS PUB 88

Encryption

FIPS PUB 46-1

FIPS PUB 74

FIPS PUB 81

FIPS PUB 113

SPEC PUB 500-54

SPEC PUB 500-61

SPEC PUB 500-156

Evaluation of Computer Security

FIPS PUB 102

SPEC PUB 500-57

SPEC PUB 500-109

SPEC PUB 500-153

NBSIR 86-3386

General Computer Security

FIPS PUB 39

FIPS PUB 73

FIPS PUB 112

SPEC PUB 500-120

SPEC PUB 500-137

SPEC PUB 500-157

SPEC PUB 500-158

Physical Security

FIPS PUB 31

Power, Grounding (Life Safety)

FIPS PUB 94

Privacy

FIPS PUB 41

SPEC PUB 500-50

Risk Management

FIPS PUB 31

FIPS PUB 65

Software and Operating Systems

SPEC PUB 500-67

SPEC PUB 500-121

SPEC PUB 500-134

User Authenticity

FIPS PUB 48

FIPS PUB 83

Network Security

SPEC PUB 500-54

The foregoing address an impressive array of complex issues which present even large, sophisticated data centers with compliance problems. If it can be assumed that data centers processing classified data are the most security conscious, then the experiences reported by the Defense Industrial Security Program (DISP) about them probably significantly understates conditions to be found at sites processing unclassified (CALS technical) data. This includes data which is procurement sensitive and contractor proprietary. Keep in mind that DISP does not address unclassfied contractor data processing systems, which are likely to be less concerned with security, when viewing the ten most common ADP security problems encountered by it listed below:

"1. System not approved for classified processing prior to use.

2. System not operating as documented, i.e., major changes made without notification to the facility security officer or DIS. Systems must also be reapproved after relocation, and users are often unaware of this requirement.

3. Storage media (diskettes, tapes, etc.) not properly marked or brought into accountability. (Example: Document created on word-processing equipment has been finalized and given a control number. But the floppy used on the WP is carried as a working diskette and never brought into accountability.)

4. Procedures are not established or not followed for deletion or destruction of information on ADP storage media. Electronic copies of documents retained (often inadvertently) when paper copies are destroyed, e.g., after completion of a classified contract. Emergency destruction procedures for fixed or damaged disks are often inadequate or non-existent.

5. Access records ("audit trails") not being properly generated, reviewed, or maintained--often because users are unaware of the importance of audit trails or the need to provide complete information.

6 .System located in an area without proper controls to deny visual access.

7. Operating system and application software not properly protected.

8. Printouts of program listings or reports not properly marked.

9. Failure to follow system upgrading or downgrading procedures outlined in the ADP/SPP.

10. Obvious lack of security education on the part of the users/operators. Personnel not aware of their security responsibilities or even that a document such as the ADP/SPP exists.

Note, first of all, that these are almost solely non-technical problems. The average facility security officer, even one without a technical ADP background, could identify and correct any of these discrepancies during the normal self-inspection which a facility conducts midway between regularly scheduled DIS inspections."[7]

1. Computer Security, *Security Awareness Bulletin, June 1986/Number 3-86, Defense Investigative Service/Defense Security Institute, Richmond, Virginia*

2. Selected Electronic Funds Transfer Issues - Privacy, Security and Equity, *March 1982, Office of Technology Assessment, Washington, D.C.*

3. Department of Defense Computer-aided Acquisition and Logistics Support (CALS) Program Implementation Guide, *MIL-HDBK-59, 20 December 1988, Washington, D.C. 20301*

4. User's Needs Drive CALS Effort, *Government Computer News, 15 May, 1989, Ziff-Davis Publishing Company, New York, New York*

5. DoD Trusted Computer System Evaluation Criteria, *DoD-5200.28-STD, December 1985, Department of Defense, Washington, D.C.*

6. Computer Security Publications: NBS Publications List 91, *February 1989, U.S. Department of Commerce, National Institute of Standards and Technology, National Computer Systems Laboratory, Gaithersburg, Maryland*

7. Weak Links: ADP Security Deficiencies, *Security Awareness Bulletin, September 1986/Number 5-86, Defense Investigative Service/Defense Security Institute, Richmond, Virginia*

5.0 CURRENT RELEVANT SECURITY INITIATIVES

The notoriety and media coverage given the computer virus and the West German hackers this past Winter have heightened general concerns about security in unclassified systems, but, in fact, the Government's concerns have been building for some time. The Department of Defense established the Defense [now National] Computer Security Center in January 1981 to advance the widespread availability of trusted computer systems. The Congress passed the Computer Security Act of 1987. This law focused the attention of federal agencies on computer security by requiring them to prepare and submit security plans for sensitive but unclassified systems to the National Institutes of Standards and Technology [formerly the National Bureau of Standards] and the National Security Agency [host to DoD's National Computer Security Center]. The computer virus and the West German hacker cases occurred well after the Government's initial actions, but, "...finally, after 15, 16 years, people are starting to pay attention".[1]

5.1 Computer Security Act of 1987

"The Computer Security Act of 1987 was passed to increase the security of unclassified systems, and though many agencies have responded with compliance plans, the measure of its success will be how well agencies comply with the legislation long term....agencies used to have a laissez-faire attitude, even though the Defense Department discovered in the 1970s that many systems could be penetrated easily".[2] The Act defines sensitive data as that whose "loss, misuse or unauthorized access to or modification....could adversely effect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under [the Privacy Act]."[3] The Act does not address information or systems which are officially classified for purposes of national defense. "The definition is intended to encompass systems that require the following:

> Confidentiality. Examples are payroll/personnel systems and systems with timed or controlled dissemination such as crop data reporting.
>
> Integrity. These systems, such as funds - transfer systems, contain data that must be protected from unauthorized modification.
>
> Availability. The systems must be available on a timely basis to meet mission requirements or to avoid losses."[3]

Under the Act, the National Institute for Standards and Technology (NIST) has responsibility for establishing standards for security of civilian agency systems, with technical advisory support from the National Security Agency. NIST has established a National Computer Systems Laboratory. The new Director's "first [act] was to plan the first meeting of the Computer System Security and Privacy Board....the 12-member board is responsible for developing standards and guidelines."[4] "One chief concern is money, Congress gave the National Institute for Standards and Technology a $3 million budget for its security program. But Raymond G. Kammer, Jr., acting director of NIST, has testified before Congress that $3 million will only begin to scratch the surface on the computer security program called for by the law."[5] "In September [1988], the General Accounting Office told Congress nearly 54,000 systems had been identified as requiring security plans. That total did not include systems at the Department of Energy, Agriculture, Interior and Health and Human Services, and the Veteran's Administration."[4]

NIST is also sponsoring and coordinating the establishment of anti-virus response centers as "a response to the computer virus attack last year involving the Defense Data Network and ARPANET....[to] provide authentic solutions....involving unclassified material throughout the Federal Government and provide common services and communications among individual response centers. Because viruses tend to occur within specific technological environments, NIST will urge agencies to establish a 'network of response centers, each servicing a different use or technological constituency'....The Computer Emergency Response Team Center at the Defense Advanced Research Projects Agency, which has been open for about a month, will serve as a prototype for other centers."[6]

5.2 National Computer Security Center

"During the 1970s, the Air Force, Advanced Research Projects Agency (ARPA), and other defense agencies undertook to develop and demonstrate solution approaches for the technical problems in resource and information-sharing computer systems. In 1977, the DoD Computer Security Initiative was started....As a culmination of these efforts, the Director of the National Security Agency was assigned responsibility for computer security for the DoD, which resulted in the DoD [now National] Computer Security Center (CSC) being formed in January 1981."[7]

The function of NCSC is to evaluate the technical protection capabilities of industry and Government-developed systems in accordance with published criteria or standards. These standards are promulgated as DoD Trusted Computer System Evaluation Criteria.[8] Vendors submit their products for specific testing to determine a product's compliance with a pre-specified (or targeted) rating classification. "This criteria classifies systems into four hierarchical divisions (D, C, B, and A - see Figure 5-1) of increased security protection and provides the basis for testing the effectiveness of security controls built into the products. Within each class are two types of security requirements, assurance and feature requirements. Assurance requirements provide confidence that the required features are there and functioning as intended. The objectives of the criteria are to provide:

A measure to assess the degree of trust that can be placed in a system,

Guidance to developers of these systems, and

A foundation for security requirements.

The NCSC, with their evaluation team, receives vendor-supplied evidence, sufficient training, test facilities, and technical assistance to allow them to accurately review, analyze, validate, examine, and test the design and implementation of the system as required by the Criteria. All this is at no cost to the Government."[7] Figures 5-1 and 5-2 summarize the criteria classifications and feature requirements. These criteria were recently clarified by the issuance of Computer Security Subscription Interpretation of the Trusted Computer System Evaluation Criteria.[9]

"The Evaluated Products for Trusted Computer Systems (called the Evaluated Products List) is contained in the Products and Services List that is prepared and published quarterly by the National Computer Security Center."[10] "By the end of 1990, 75 products will be on the Evaluated Products List."[2] Whereas most of the products currently on the EPL are computer operating systems or add-on access or data transfer encryption features (see Appendix B for the most recent EPL), the ORACLE[11], and Trudata Model 3BBL[12] data base management systems (DBMS) are currently in evaluation or testing. Sybase, Inc.'s "...*Secure SQL Server* is the first commercial relational data base management system (RDBMS) designed to meet the National Computer Security Center's B1 and B2 levels of security for multilevel data.[13] The DBMS category of products are essential to the protection of both Government and industry (sensitive and proprietary, respectively) data in an unclassified CALS technical data environment.

DoD has mandated that all DoD-component automated information systems processing sensitive unclassified information must achieve classification level C2 by 1992.[14]

As part of its Low Cost Encryption and Authentication Devise (LEAD) Project, the NSA is also developing a personal computer card (i.e., a 2K EEPROM smart card) authentication medium for access to the Defense Data Network (DDN). Contractors currently involved in this effort are Personal Computer Card Corporation, Mitre Corporation, ACS Communications, Inc. and Codercard, Inc., to name but a few. Estimates for the implementation of this access authentication scheme involve the issuance of from 650,000 to 1,500,000 "smart" cards. The same technology is currently being deployed as access keys for the DoD secure voice (STU-III) telephone system. This technology, in conjunction with a certified DBMS, has much to offer operators of CALS data host systems to appropriately protect unclassified data, both Government restricted/sensitive and contractor proprietary.[15] The NCSC also has under evaluation a fingerprint data security access device which extends security to the computer application transaction level which would be synergistic with DBMS file data access security features.[16]

5.3 CALS ISG Protection and Integrity Task Group

The DoD CALS Policy Office has impaneled an Industry Steering Group (ISG) for Data Protection and Integrity (DP&I) to assist in clarifying security issues and developing guidelines for participants in weapon system programs employing CALS. The Task Group "...reviewed a draft DoD CALS security directive and as a result, reorganized. The directive, Computer-aided Acquisition and Logistics Support Data Protection and Security Policy Directive, was drafted by Dr. Ruth Davis, President of Pymaturing Group, Inc., advisors to the DoD CALS Policy Office.

Three new subgroups have been established:

1. Data Classification Management, chaired by Harry Brewer of Rockwell, TEL 213-414-4255, will evaluate methods of identifying data for secure protection.

2. System Security Engineering, chaired by Bennett C. Carp of AT&T, TEL 201-949-0699, will apply system security engineering methodology to CALS requirements, standards and architectures to identify threats and vulnerabilities.

Trusted Computer System Evaluation Criteria: Classification Summary

Division D-Minimal Protection

This division contains one class for evaluated systems that fail to meet the requirements of a higher class.

Division C-Discretionary Protection

This division provides (need-to-know) protection and accountability of subjects, and the actions they initiate through audit capabilities.

Class C1:

The Trusted Computing Base (TCB) provides separation of users and data. It incorporates some form of credible controls to enforce access limitation on an individual basis. Class C1 environment is one of cooperating users processing data at the same levels of sensitivity.

Class C2:

Systems in this class enforce a more finely grained discretionary access control, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Division B-Mandatory Protection

A major requirement is a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules. Systems must carry the sensitivity labels with major data structures in the system. The reference monitor concept must be implemented.

Class B1:

An informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

Class B2:

The TCB is based on a formal security policy model that extends control to all subjects and objects in the ADP system. Covert channels are addressed. The TCB must be structured into protection-critical and nonprotection-critical elements. The TCB interface is well-defined. Authentication mechanisms are strengthened, and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class B3:

The Class B3 TCB must satisfy the reference monitor that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. The TCB is structured to exclude code not essential to security policy enforcement. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Division A-Verified Protection

Class A1:

A1 systems have no additional architectural features or policy requirements are added. The distinguishable feature is the analysis derived from formal design specification and verification techniques, and the resulting high degree of assurance that the TCB is correctly implemented. The assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. There are five important criteria for Class A1 design verification:

1. A formal model of the security policy must be clearly identified and documented, including a mathematical proof that it is consistent with its axioms and can support the security policy.

2. An FTLS must be produced that includes abstract definitions of the functions the TCB performs and of the hardware and/or firmware mechanisms used to support separate execution domains.

3. The FTLS of the TCB must be consistent with the model by formal techniques where possible and informal ones otherwise.

4. The TCB implementation is informally shown to be consistent with the FTLS. The elements of the FTLS, using informal techniques, must correspond to the elements of the TCB. The FTLS must express the unified protection mechanism required to satisfy the security policy, and it is the elements of this protection mechanism that are mapped to the elements of the TCB.

5. Formal analysis techniques are used to identify and analyze covert channels. Informal techniques may be used to identify covert timing channels. The continued existence of identified covert channels in the system must be justified.

FIGURE 5-1

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA SUMMARY CHART

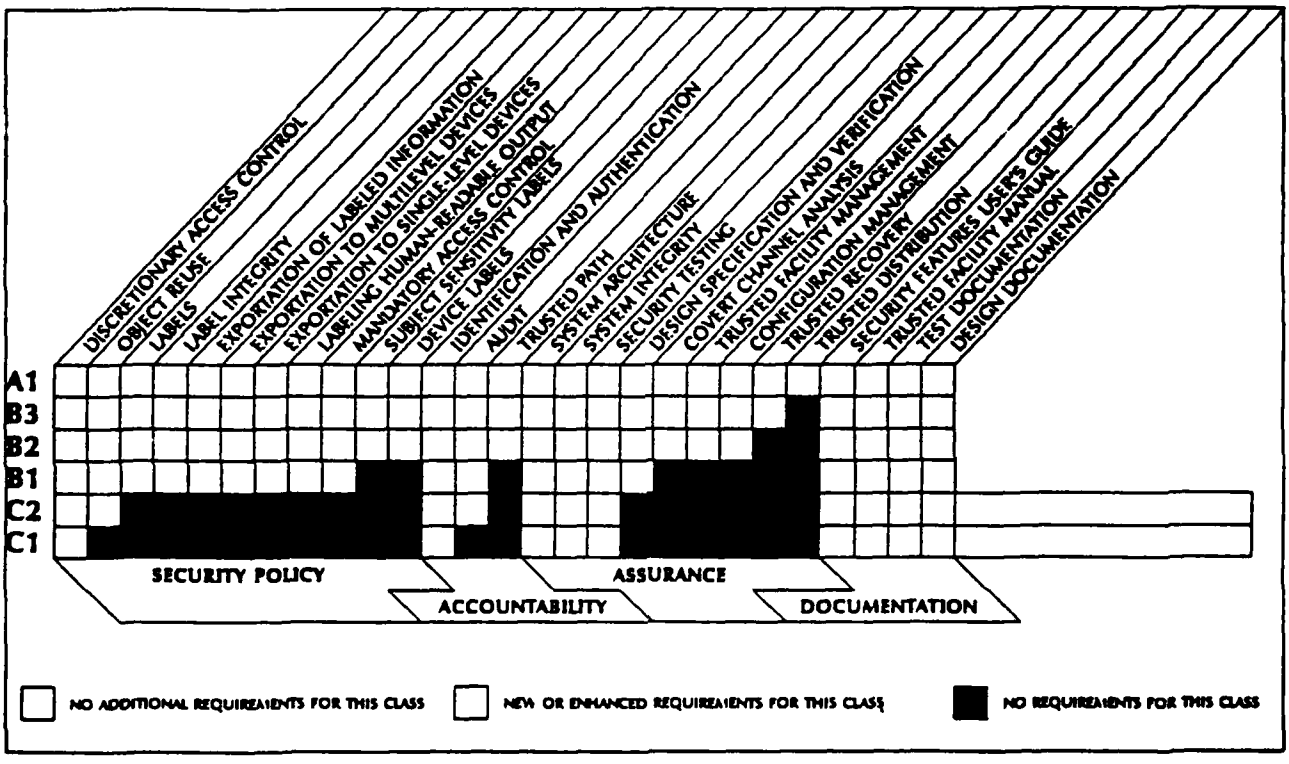


FIGURE 5-2

3. Electronic Information Security, chaired by Ronald A. Martin of Hughes, TEL 213-607-1998, will evaluate operational, legislative and other issues and develop audit procedures and security safeguards for data.

A fourth subgroup is planned for Operations Security and [a fifth subgroup] Configuration Integrity Management is [also] planned. A special position report on Rights in Technical Data and Computer Software has been prepared by DP&I Task Group (TG) Chair William D. Jascomb of Lockheed - Georgia, TEL 404-424-2625.

The DP&I Task Group has added a third chairperson, Ralph D. Clark of TRW. Clark joins William Jascomb and Howard E. Chambers of Rockwell.

The reorganization of the DP&I TG reflects a new awareness in the ISG of how pervasive security issues will be in CALS. Normal security practices guard mixed Government and contractor data from disruption and theft. However, CALS implies levels of access unforeseen by most security and interoperability standards (see CALS Report, October, 1988). In addition, contractors are sensitive to loss of proprietary data and software rights to the Armed Services preparing for rapid acquisition of parts from comprehensive product data models (see CALS Report, January, 1989).

It is also clear that DP&I will require cultural changes. The Davis draft policy tries to strike a delicate balance of modifications to existing security and management practices. It describes a hierarchy of Risk Approval Authorities (RAA's) and procedures that would complement existing Executive Agency (EA) Designated Approval Authority (DAA) procedures for reviewing computer security issues. The RAA structure would control use of compartmented, multi-EA, or multilevel security information. Although few familiar with the problem question the need for new controls, the proper organization to achieve them will be the subject of considerable debate."[17]

1. Computer Security: Concerns Fuel Job Growth, *the Washington Post, 7 May 1989, The Washington Post Company, Washington, D.C.*

2. Long-Term Results of Security Act Are What Count, *Government Computer News, 1 May 1989, Ziff-Davis Publishing Company, New York, New York*

3. OMB Faults DoD Compliance With Computer Security Act, *Federal Computer Week, 10 April 1989, Federal Computer Week Publishing, Inc., Fails Church, Virginia*

4. NIST Gets 2,000 Agency Security Plans for Study, *Government Computer News, 6 February 1989, Ziff-Davis Publishing Company, New York, New York*

5. 101st Congress Deals With New Faces, Old Issues, *Government Computer News, 23 January 1989, Ziff-Davis Publishing Company, New York, New York*

6. NIST to Coordinate Anti-Virus Response Centers, *Government Computer News, 20 March 1989, Ziff-Davis Publishing Company, New York, New York*

7. Overview of Department of Defense Computer Security Guidelines, *Information Security Volumes, 80-400-101/111, June 1985, DATAPRO Research Corporation, Delran, New Jersey*

8. DoD Trusted Computer System Evaluation Criteria, *DoD-5200.28-STD, December 1985, Department of Defense, Washington, D.C.*

9. Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria, *January 1989, National Computer Security Center, National Security Agency, Fort Meade, Maryland*

10. Department of Defense Computer-aided Acquisition and Logistics Support (CALS) Program Implementation Guide, *MIL-HDBK-59, 20 December 1988, Washington, D.C. 20301*

11. NSA Aids Oracle In Research On DBMS Security, *Government Computer News, 23 January 1989, Ziff-Davis Publishing Company, New York, New York*

12. NCS Evaluating Multilevel Database Security Product, *Government Computer News, 23 January 1989, Ziff-Davis Publishing Company, New York, New York*

13. B1, B2, Bingo, *Information Center, September 1989, Boston, Massachusetts*

14. Security Requirements for Automated Information Systems (AISs) *Department of Defense Directive 5200.28, 21 March 1988, Washington, D.C.*

15. Commercial Exposure of Products (2K Byte Product), *11 March 1989, Personal Computer Card Corporation, New York, New York*

16. Fingerprint ID System Not Just for Spooks, *Government Computer News, 12 June 1989, Ziff-Davis Publishing Company, New York, New York*

17. CALS ISG Data Protection & Integrity TG Reviews New Policy, Reorganizes, *CALS Report, February 1989, Knowledge Base International, Houstin, Texas*

APPENDIX A

GOVERNMENT COMPUTER SECURITY PUBLICATIONS

"Computer security is important to managers and users of information systems. Security is the tool for achieving integrity and accuracy of data, confidentiality of information handled by systems, and the availability of systems, data, and services. Many different accidental and intentional events can threaten security. ICST (Institute for Computer Science and Technology) identifies and develops cost-effective methods to protect computers and data against all types of losses. These methods include technical solutions to computer security problems, as well as sound management practices.

How to Order Publications

These publications are available through the Government Printing Office (GPO) and the National Technical Information Service (NTIS). The source and price for each publication are indicated. Orders for publications should include title of publication, NBS publication number (Spec. Pub. 000, Tech. Note 000, etc.) and NTIS or GPO number. You may order at the price listed; however, prices are subject to change without notice.

Submit payment in the form of postal money order, express money order or check made out to the Superintendent of Documents for GPO-stocked documents or to the National Technical Information Service for NTIS-stocked documents.

Mailing addresses are:

Superintendent of Documents

U.S. Government Printing Office

Washington, D.C. 20402

National Technical Information Service

5285 Port Royal Road

Springfield, VA 22161

Telephone numbers for information are:

GPO Order Desk (202) 783-3238

NTIS Orders (703) 487-4780

NTIS Information (703) 487-4600

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS)

Federal Information Processing Standards Publications (FIPS PUBS) are developed by the Institute for Computer Sciences and Technology (ICST) and issued under the provisions of the Federal Property and Administrative Services Act of 1949, as amended; Public Law 89-306 (79 Stat. 1127); Executive Order 11717 (38 FR 12315); and Part 6 of Title 15 of the Code of Federal Regulations (CFR).

FIPS PUBS are sold by the National Technical Information Service (NTIS), U.S. Department of Commerce. A list of current FIPS covering all ICST program areas is available from:

Standards Processing Coordinator (ADP)

Institute for Computer Sciences and Technology

Technology Building, B-64

National Bureau of Standards

Gaithersburg, MD 20899

Phone: (301) 975-2817

FIPS PUB 31 GUIDELINES FOR ADP PHYSICAL SECURITY AND RISK MANAGEMENT

June 1974

Provides guidance to Federal organizations in developing physical security and risk management programs for their ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans security awareness, and security audit. Can be used as a checklist for planning and evaluating security of computer systems.

FIPS PUB 39 GLOSSARY FOR COMPUTER SYSTEMS SECURITY

February 1974

A reference document containing approximately 170 terms and definitions pertaining to privacy and computer security.

FIPS PUB 41 COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

May 1975

Provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. Discusses categories of risks and related safeguards for physical security, information management practices, and systems controls to improve system security.

FIPS PUB 46-1 DATA ENCRYPTION STANDARD

January 1988 (Reaffirmed until 1992)

Specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of sensitive, but unclassified, computer data. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher and the steps required to transform the cipher back to its original form. This standard has been adopted as a voluntary industry standard ANSI X3.92-1981/R1987

FIPS PUB 48 GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION

April 1977

Discusses the performance of personal identification devices, how to evaluate them and considerations for their use within the context of computer system security.

FIPS PUB 65 GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS

August 1979

Presents a technique for conducting a risk analysis of an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency caused by adverse events. This guideline describes the characteristics and attributes of a computer system that must be known for a risk analysis and gives an example of the risk analysis process.

FIPS PUB 73 GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS

June 1980

Describes the different security objectives for a computer application, explains the control measures that can be sued, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection. Fundamental security controls such as data validation, journalling, variance detection, and encryption are discussed.

FIPS PUB 74 GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD

April 1981

Provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46 and FIPS PUB 81.

FIPS PUB 81 DES MODES OF OPERATION

December 1980

Defines four modes of operation for the Data Encryption Standard which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically occurrence and the damage protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

FIPS PUB 83 GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL

September 1980

Provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.

FIPS PUB 87 GUIDELINES FOR ADP CONTINGENCY PLANNING

March 1981

Describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

FIPS PUB 88 GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN DATABASE APPLICATIONS

August 1981

Provides explicit advice on achieving database integrity and security control. Identifies integrity and security problems and discusses procedures and methods which have proven effective in addressing these problems. Provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.

FIPS PUB 94 GUIDELINE ON ELECTRICAL POWER FOR ADP INSTALLATIONS

September 1982

Provides information on factors in the electrical environment that affect the operation of ADP systems. Describes the fundamentals of power, grounding, life-safety, static electricity, and lightning protection requirements, and provides a checklist for evaluating ADP sites.

FIPS PUB 102 GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION

September 1983

Describes how to establish and how to carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process.

FIPS PUB 112 STANDARD ON PASSWORD USAGE

May 1985

This standard defines ten factors to be considered in the design, implementation and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems which must meet higher security requirements.

FIPS PUB 113 STANDARD ON COMPUTER DATA AUTHENTICATION

May 1985

This standard specifies la Data Authentication Algorithm (DAA) which, when applied to computer data, automatically and accurately detects unauthorized modifications, both intentional and accidental. Based on the Data Encryption Standard (DES), this standard is compatible with requirements adopted by the Department of Treasury and the banking community to protect electronic fund transfer transactions.

Special Publications and Other Reports

These publications present the results of ICST studies, investigations, and research on computer security and risk management issues. Publications are sold by either the Government Printing Office or the National Technical Information Service.

NBS SPEC PUB 500-54 - A KEY NOTARIZATION SYSTEM FOR COMPUTER NETWORKS

By Miles E. Smid

October 1979

Describes a system for key notarization, which can be used with an encryption device, to improve data security in computer networks. The key notarization system can be used to communicate securely between two users, communicate via encrypted mail, protect personal files, and provide a digital signature capability.

NBS SPEC PUB 500-57 - AUDIT AND EVALUATION OF COMPUTER SECURITY II: SYSTEM VULNERABILITIES AND CONTROLS

Edited by Zella G. Ruthberg

April 1980

Proceedings of the second NBS/GAO workshop to develop improved computer security audit procedures. Covers eight sessions: three sessions on managerial and organizational vulnerabilities and controls and five technical sessions on terminals and remote peripherals, communication components, operating systems, applications and non-integrated data files, and data base management systems.

NBS SPEC PUB 500-61 - MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD

By Jason Gait

August 1980

Describes four tests that can be used by manufacturers and users to check the operation of data encryption devices. These tests are simple, efficient, and independent of the implementation of the Data Encryption Standard (FIPS 46).

NBS SPEC PUB 500-67 - THE SRI HIERARCHICAL DEVELOPMENT METHODOLOGY (HDM) AND ITS APPLICATION TO THE DEVELOPMENT OF SECURE SOFTWARE

By Karl N. Levitt, Peter Neumann, and Lawrence Robinson

October 1980

Describes the SRI Hierarchical Development Methodology for designing large software systems such as operating systems and data management systems that must meet stringent security requirements.

NBS SPEC PUB 500-85 - EXECUTIVE GUIDE TO ADP CONTINGENCY PLANNING

By James K. Shaw and Stuart W. Katzke

July 1981

This document provides, in the form of questions and answers, the background, and basic essential information required to understand the developmental process for automatic data processing (ADP) contingency plans. The primary intended audience consists of executives and managers who depend on ADP resources and services, yet may not be directly responsible for the daily management or supervision of data processing activities or facilities.

NBS SPEC PUB 500-109 - OVERVIEW OF COMPUTER SECURITY CERTIFICATION AND ACCREDITATION

By Zella G. Ruthberg and William Neugent

April 1984

This publication is a summary of and a guide to FIPS PUB 102, Guideline to Computer Security Certification and Accreditation. It is oriented toward the needs of ADP policy managers, information resource managers, ADP technical managers, and ADP staff in understanding the certification and accredition process.

NBS SPEC PUB 500-120 - SECURITY OF PERSONAL COMPUTER SYSTEMS - A MANAGEMENT GUIDE

By Dennis D. Steinauer

January 1985

This publication provides practical advice on the following issues: physical and environmental protection system and data access control; integrity of software and data; backup and contingency planning; auditability; communications protection. References to additional information, a self-audit checklist, and a guide to security products for personal computers are included in the appendices.

NBS SPEC PUB 500-121 - GUIDANCE ON PLANNING AND IMPLEMENTING COMPUTER SYSTEMS RELIABILITY

By Lynne S. Rosenthal

January 1985

This report presents guidance to managers and planners on the basic concepts of computer system reliability and on the implementation of a management program to improve system reliability. Topics covered include techniques for quantifying and evaluating data to measure system reliability, designing systems for reliability, and recovery of a computer system after it has failed or produced erroneous output. An appendix contains references and a list of selected readings.

NBS SPEC PUB 500-133 - TECHNOLOGY ASSESSMENT; METHODS FOR MEASURING THE LEVEL OF COMPUTER SECURITY

By William Neugent, John Gilligan, Lance Hoffman, and Zella G. Ruthberg

October 1985

The document covers methods for measuring the level of computer security, i.e. technical tools or processes which can be used to help establish positive indications of security adequacy in computer applications, systems, and installations. The report addresses individual techniques and approaches, as well as broader methodologies which permit the formulation of a composite measure of security that uses the results of these individual techniques and approaches.

NBS SPEC PUB 500-134 - GUIDE ON SELECTING ADP BACKUP PROCESS ALTERNATIVES

By Irene Isaac

November 1985

Discusses the selection of ADP backup processing support in advance of events that cause the loss of data processing capability. Emphasis is placed on management support at all levels of the organization for planning, funding, and testing of an alternate processing strategy. The alternative processing methods and criteria for selecting the most suitable method are presented, and a checklist for evaluating the suitability of alternatives is provided.

NBS SPEC PUB 500-137 - SECURITY FOR DIAL-UP LINES

By Eugene F. Troy

May 1986

Ways to protect computers from intruders via dial-up telephone lines are discussed in this guide. Highlighted are hardware devices which can be fitted to computers or used with their dial-up terminals to provide communications protection for non-classified computer systems. Six different types of hardware devices and the ways that they can be used to protect dial-up computers communications are described. Also discussed are techniques that can be added to computer operating systems or incorporated into system management or administrative procedures.

NBS SPEC PUB 500-153 - GUIDE TO AUDITING FOR CONTROLS AND SECURITY: A SYSTEM DEVELOPMENT LIFE CYCLE APPROACH

Editors/Authors: Zella G. Ruthberg, Bonnie T. Fisher, William E. Perry, John W. Lainhart IV, James G. Cox, Mark Gillen, and Douglas B. Hunt

April 1988

This guide describes a process for auditing the system development life cycle (SDLC) of an automated information system (AIS) to ensure that controls and security are designed and built into the system. The guide was developed by the Electronic Data Processing (EDP) Systems Review and Security Work Group of the Computer Security Project within the President's Council on Integrity and Efficiency (PCIE), and contains bibliographies, and a description of pertinent laws and regulations.

NBS SPEC PUB 500-156 - MESSAGE AUTHENTICATION CODE (MAC) VALIDATION SYSTEM: REQUIREMENTS AND PROCEDURES

By Miles Smid, Elaine Barker, David Balenson and Martha Haykin

May 1988

Describes the Message Authentication Code (MAC) Validation System (MVS) which was developed by NBS to test message authentication devices for conformance to two data authentication standards (including FIPS 113). This publication describes the basic design and configuration of the MVS, and the requirements and administrative procedures to be followed for requesting validations.

NBS SPEC PUB 500-157 - SMART CARD TECHNOLOGY: NEW METHODS FOR COMPUTER ACCESS CONTROL

By Marty Haykin and Robert Warnar, August 1988

This document describes the basic components of a smart card and provides background information on the underlying integrated circuit technologies. The capabilities of a smart card are discussed, especially its applicability for computer security. The report describes research being conducted on smart card access control techniques; other major U.S. and international groups involved in the development of standards for smart cards and related devices are outlined in the appendix.

NBSIR 86-3386 - WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW

By Zella Ruthberg and Bonnie Fisher

August 1986

This publication describes a methodology for prioritizing the work performed EDP auditors and computer security reviewers. Developed at an invitational workshop attended by government and private sector experts, the work plan enables users to evaluate computer systems for both EDP audit and security review functions and to develop a measurement of the risk of the systems. Based on this measure of risk, the auditor can then determine where to spend review time."[1]

Price List[1]

PUBLICATION	ORDERING NUMBER	PRICE
FIPS PUB 31	FIPS PUB 31	$11.95
FIPS PUB 39	FIPS PUB 39	$ 9.95
FIPS PUB 41	FIPS PUB 41	$ 9.95
FIPS PUB 46-1	FIPS PUB 46-1	$ 9.95
FIPS PUB 48	FIPS PUB 48	$ 9.95
FIPS PUB 65	FIPS PUB 65	$ 9.95
FIPS PUB 73	FIPS PUB 73	$11.95
FIPS PUB 74	FIPS PUB 74	$ 9.95
FIPS PUB 81	FIPS PUB 81	$ 9.95
FIPS PUB 83	FIPS PUB 83	$ 9.95
FIPS PUB 87	FIPS PUB 87	$ 9.95
FIPS PUB 88	FIPS PUB 88	$11.95
FIPS PUB 94	FIPS PUB 94	$16.95
FIPS PUB 102	FIPS PUB 102	$11.95
FIPS PUB 112	FIPS PUB 112	$11.95
FIPS PUB 113	FIPS PUB 113	$ 9.95
SPEC PUB 54	PB 80104698	$11.95
SPEC PUB 57	SN 003-003-02178-4	$ 7.00
SPEC PUB 61	PB 80221211	$ 9.95
SPEC PUB 67	PB 81115537	$13.95
SPEC PUB 85	PB 82165226	$ 9.95
SPEC PUB 109	SN 003-003-02567-4	$ 1.50
SPEC PUB 120	SN 003-003-02627-1	$ 3.00
SPEC PUB 121	SN 003-003-02628-0	$ 2.25
SPEC PUB 133	SN 003-003-02686-7	$ 8.00
SPEC PUB 134	SN 003-003-02701-4	$ 1.75
SPEC PUB 137	PB 86213097	$13.95

PUBLICATION	ORDERING NUMBER	PRICE
SPEC PUB 153	SN 003-003-02856-8	$13.00
SPEC PUB 156	SN 003-003-02860-6	$ 2.75
SPEC PUB 157	SN 003-003-02887-8	$ 2.75
SPEC PUB 158	SN 003-003-02883-5	$ 7.50
NBSIR 86-3386	PB 86247897	$11.95

FIPS Available from NTIS

SN Numbers - Stocked by GPO

PB Numbers - Stocked by NTIS

1. Computer Security Publications, NBS Publications List 91, *February 1989, National Institute of Standards and Technology, National Computer Systems Laboratory, Gaithersburg, Maryland.*

APPENDIX B

NCSC EVALUATED PRODUCT LIST[1]

GENERAL-PURPOSE OPERATING SYSTEMS:	OVERALL EVALUATION CLASSIFICATION
Secure Communications Processor (SCOMP) - STOP Release 2.1 - CSC-EPL-85/001	A1
Multics - MR11.0 - CSC-EPL-85/003	B2
Network Operating System (NOS) - Security Evaluation Package Version 2.2 - CSC-EPL-86/003	C2
VAX/VMS - Version 4.3, with September Systems Dispatch article 95.5.8, V4 Security Update and accompanying letter - CSC-EPL-86/004	C2
UTX/32S - Release 1.0 - CSC-EPL-86/007	C2
A Series MCP/AS with InfoGuard Security Enhancements - Release 3.7 - CSC-EPL-87/003	C2
Automatic Control Facility 2 (acf2) - Release 3.1 - CSC-EPL-87/007	C2
MVS/XA with RACF - Version 1.8 - CSC-EPL-88/003	C2
Primos - Revision 2.1.0.1 DODC2A - CSC-EPL-88/009	C2
MPE V/E - Release G.03.04 with patch AV92 - CSC-EPL-88/0010	C2
AOS/VS Rev. 7.60 - CSC-EPL-89/001	C2
ADD-ON PACKAGES:	
Resource Access Control Facility (RACF) - Version 1 Release 5 - CSC-EPL-84/001 (as of July 1989)	C1
Access Control Facility 2 (ACF2) - Releases 3.1.3 through 4.0 - CSC-EPL-84/002	C2
Top Secret - Version 3.0 - CSC-EPL-85/002	C2

SUB-SYSTEMS:	OVERALL EVALUATION CLASSIFICATION
Gordian Systems Access Key - Release Version A.00 - CSC-EPL-86/001	D
Codercard CPP-300 Port Protector - CPP-300 - CSC-EPL-86/002	D
Watchdog PC Data Security - Version 4.1 - CSC-EPL-86/005	D
Sytek PFX - A2000/A2100 - CSC-EPL-86/006	D
Access Control Encryption (ACE) System - 1986 16 port hardware version - CSC-EPL-87/001	D
Safeword UNIX-Safe - Version 3.1 - CSC-EPL-87/002	D
Sentinel - Version 3.13 - CSC-EPL-87/004	D
SGT Security - Version 4A. - CSC-EPL-87/005	D
Triad Plus - Version 1.3 - CSC-EPL-87/006	D
SureKey - Key Concepts, Inc. - CSC-EPL-87/008	D
IDX-50 - Version 7 - CSC-EPL-88/001	D
Cortana Personal Computer Security System - Version 1.21 - CSC-EPL-88/002	D
DPS-800/12 - Spectrum Manufacturing, Inc. - CSC-EPL-88/004	D
DIALBACK - Version 1.5 - CSC-EPL-88/005	D
Private Access - Model L20 - CSC-EPL-88/007	D

1. Information Systems Security Products and Services Catalogue, *July 1989, National Security Agency, Fort George C. Meade, Maryland.*

APPENDIX C

ACRONYMS

ADP/T - Automatic Data Processing and Telecommunications

ADP - Automatic Data Processing

ANSI - American National Standards Institute

ARPANET - Advanced Research Projects Agency Network

ASO - Aviation Supply Office

BAA - Business Area Analysis

C3 - Command, Control, and Communication

CAD - Computer Aided Design

CAE - Computer Aided Engineering

CALS - Computer-aided Acquisition and Logistics Support

CAM - Computer Aided Manufacturing

CASREPT - Casualty Report

CBE - Critical Baseline Enhancements

CGM - Computer Graphics Metafile

CINC - Commander in Chief

CITIS - Contractor Integration Technical Information System

COMMIT - Communications Intelligence

CSC - Computer Security Center

DAA - Designated Approval Agency

DBMS - Data Base Management System

DCAA - Defense Contracts Audit Agency

DCASR - Defense Contract Administration Region

DCIS - Defense Criminal Investigation Service

DDN - Defense Data Network

DESC - Defense Electronic Supply Center

DIDS - Defense Integrated Data Systems

DISP - Defense Industrial Security Program

DLA - Defense Logistics Agency

DLSC - Defense Logistics Services Agency

DoD - Department of Defense

DP&I - Data Protection and Integrity

DSC - Defense Supply Center

DSSSL - Document Style Semantics and Specification Language

EA - Executive Agency

EDI - Electronic Data Interchange

EDMICS - Engineering Data Management Information Control

EPL - Evaluated Products List

ESCN - Electronic Supplier/Customer Network

FIPS - Federal Information Processing Standard

FORSTAT - Force Status

GSA - Government Servics Administration

IEEE - Institute of Electrical and Electronic Engineers

IGES - Initial Graphics Interchange Standard

IPP - Industrial Preparaedness Planning

ISG - Industry Steering Group

ISO - International Standards Organization

IWSDB - Integrated Weapon System Data Base

JCS - Joint Chiefs of Staff

LEAD - Low Cost Encryption and Authentication Device

LSMP - Logistics Systems Modernization Program

MEDALS - Military Engineering Data Asset Locator System

MILS - Military Standard Logistics System

MILSTRIP - Military Standard Requisitioning and Issue Procedures

MODELS - Modernization of Defense Logistics Standard Systems

NASA - National Aeronautics and Space Administration

NATO - North Atlantic Treaty Organization

NBS - National Bureau of Standards

NCSC - National Computer Security Center

NIST - National Institute for Standards and Technology

NMCS - Not Mission Capable Supply

NORAD - North Air Defense

NRC - National Research Council

NSDD - National Security Decision Directive

ODA - Office of Document Architecture

OPTIMIS - Operations Management Information System

OSD - Office of the Secretary of Defense

OSI - Open System Interconnection

PC - Personal Computer

PDES - Product Data Exchange Specification

RAA - Risk Approval Authority

RFQ - Request For Quotation

SDI - Strategic Defense Initiative

SGML - Standard Generalized Makeup Language

SGML - Standard Generalized Markup Language

SQL - Standard Query Language

STD - Standard

TCP/IP - Transmission Control Protocol/Internet Protocol

TG - Task Group

APPENDIX D

SECURITY DIRECTIVES AND REGULATIONS LIST

This Appendix provides a summary listing of directives, regulations, and guidance documents dealing with computer security.

1. A Guide to Understanding AUDIT in Trusted Systems, NCSC-TG-001-88, Version 2 - GPO stock number: 088-000-00508-7 (Tan Book)

2. A Guide to Understanding CONFIGURATION MANAGEMENT in Trusted Systems, NCSC-TG-001-88, Version 1 - GPO stock number: 008-000-00507-09 (Lt. Orange)

3. ADP Security Manual, DLA Manual 5200.1, includes changes 1-7, June 1982.

4. ADP Security Manual, DoD 5200.28-M, January 1973, authorized by DoD Directive 5200.28, December 18, 1972

5. Communications Security (COMSEC) (U), DoD Directive C-5400.5, October 6, 1981

6. Computer Security Act of 1987, Public Law 100-235, January 8, 1988.

7. Computer Security Subsystem Interpretation, NCSC-TG-009, Version 1 (Venice Blue)

8. Computer Security Technical Vulnerability Reporting Program, September 2, 1986

9. Control of Compromising Emanations (U), DoD Directive S-5200.19, February 10, 1968

10. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985, authorized by DoD Directive 5200.28, December 18, 1972

11. Discretionary Access Controls Guidelines, NCSC-TG-003-87 (Dk. Orange)

12. Distribution Statement on Technical Documents, DoD Directive 5230.24, March 18, 1987

13. DoD Personnel Security Program, DoD Directive 5200.2, December 20, 1979

14. DoD Password Management Guidelines, CSC-STD-002-85, GPO stock number: 008-000-00443-9 (Green Book)

15. DoD Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, GPO stock number: 008-000-00461-7 (Orange Book)

16. Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-003-85, GPO stock number: 008-000-00442-1 (Yellow Book 03)

17. Industrial Security Program, DoD Directive 5220.22, November 1, 1986 .

18. Industrial Security Regulation, DoD Regulation 5220.22-R, December 1985, authorized by DoD Directive 5220, December 8, 1980

19. Information Security Program Regulation, DoD 5200.1-R, June 1986, authorized by DoD Directive 5200.1, June 7, 1982

20. Internal Control Systems, OMB Circular No. A-123, 16 August 1983.

21. Internal Management Control Program, DoD Directive 5010.38, July 16, 1984

22. Life Cycle Management of Automated Information Systems (AIS), DoD Directive 7920.1, October 17, 1978

23. Management of Federal Information Resources, Office of Management and Budget Circular No. A-130, December 12, 1985

24. National Security Information, Executive Order 12356, April 6, 1982

25. PC Security Considerations, CSC-WA-002-85, GPO stock number: 008-000-00439-1 (Lt. Blue Book)

26. Safeguarding the Single Integrated Operational Plan (U), SM-313-83, May 10, 1983

27. Security of DoD Contractor Telecommunications, DoD Instruction 5210.74, June 26, 1985

28. Security Policy on Intelligence Information in Automated Systems and Networks (U), Director of Central Intelligence Directive Number 1/16, January 4, 1983.

29. Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements, CSC-STD-004-85, GPO stock number: 008-000-00441-2 (Yellow Book)

30. TEMPEST Countermeasures for Facilities Outside the United States, National Communication Security Instruction 5005, January 1, 1984.

31. TEMPEST Countermeasures for Facilities Outside the United States, National Communication Security Instruction 5004, January 1, 1984.

32. Trusted Network Interpretation, NCSC-TG-005, Version 1, (GPO stock number: 008-000-00486-2 (Red Book)

33. Trusted Network Interpretations, NCSC-TG-005, Version 1, July 31, 1987.

APPENDIX E

BIBLIOGRAPHY

1. B1, B2, Bingo, Information Center, September 1989, Boston, Massachusetts.

2. CALS Briefing will Feature Noted Speakers, Government Computer News, 17 April 1989, Ziff-Davis Publishing Company, New York, New York.

3. CALS ISG Data Protection & Integrity TG Reviews New Policy, Reorganizes, CALS Report, February 1989, Knowledge Base, International, Houstin, Texas

4. Computer-aided Acquisition and Logistic Support (CALS), Software Technology Service Bulletin, 16 December 1988, IDC Washington, Inc., Vienna, Virginia.

5. Commercial Exposure of Products (2K Byte Product), 11 March 1989, Personal Computer Card Corporation, New York, New York

6. Computer-Protection Market Grows, Thrives on Fear: Many Virus Remedies Are Only Placebos, 23 May 1989, The Washington Post, Washington, D.C.

7. Computer Security, Security Awareness Bulletin, June 1986/Number 3-86, Defense Investigative Service/Defense Security Institute, Richmond, Virginia

8. Computer Security: Concerns Fuel Job Growth, the Washington Post, 7 May 1989, The Washington Post Company, Washington, D.C.

9. Computer Security Publications: NBS Publications List 91, February 1989, U.S. Department of Commerce, National Institute of Standards and Technology, National Computer Systems Laboratory, Gaithersburg, Maryland

10. Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria, January 1989, National Computer Security Center, National Security Agency, Fort Meade, Maryland

11. Defense Logistics Agency Security Plan, 10 January 1989, Defense Logistics Agency, Alexandria, Virginia [For Official Use Only].

12. Department of Defense Computer-aided Acquisition and Logistics Support (CALS) Program Implementation Guide, MIL-HDBK-59, 20 December 1988, Washington, D.C. 20301

13. DoD Trusted Computer System Evaluation Criteria, DoD-5200.28-STD, December 1985, Department of Defense, Washington, D.C.

14. Electronics Data Interchange: Bringing it Together in Government Conference, the Defense Logistics Standard Systems Office presentation, May 26, 1988, National Bureau of Standards, Gaithersburg, Maryland

15. First Public US ODA Demonstration a Success, CALS Report, Vol. 2 No. 2, page 7, 2 February 1989, Knowledge Base International, Houston, Texas

16. Fingerprint ID System Not Just for Spooks, Government Computer News, 12 June 1989, Ziff-Davis Publishing Company, New York, New York

17. German Computer Hackers Held for Spying for Soviets, March 3, 1989, The Washington Post, Washington, D.C. [can be electronically retrieved on NEXIS through Mead Data Central].

18. Information Security, Update of Data on Employees Affected by Federal Security Programs, GAO/NSIAD-89-56FS, 7 March 1989, U.S. General Accounting Office, Washington, D.C.

19. Information Systems Security Products and Services Catalogue, July 1989, National Security Agency, Fort George G. Meade, Maryland.

20. Long-Term Results of Security Act Are What Count, Government Computer News, 1 May 1989, Ziff-Davis Publishing Company, New York, New York

21. Military Standard Requisitioning and Issue Procedures, (MILSTRIP) DoD 4000.25-1-M, May 1987, Department of Defense, Washington, D.C.

22. NCS Evaluating Multilevel Database Security Product, Government Computer News, 23 January 1989, Ziff-Davis Publishing Company, New York, New York

23. NIST Gets 2,000 Agency Security Plans for Study, Government Computer News, 6 February 1989, Ziff-Davis Publishing Company, New York, New York

24. NIST to Coordinate Anti-Virus Response Centers, Government Computer News, 20 March 1989, Ziff-Davis Publishing Company, New York, New York

25. NSA Aids Oracle In Research On DBMS Security, Government Computer News, 23 January 1989, Ziff-Davis Publishing Company, New York, New York

26. Object-Oriented Intelligence Gateways, Sandy heller (Computer Corporation of America), 29 September 1987, CALS Intelligent Gateway Conference, Planning Research Corporation, McLean, Virginia

27. OMB Faults DoD Compliance With Computer Security Act, Federal Computer Week, 10 April 1989, Federal Computer Week Publishing, Inc., Falls Church, Virginia

28. OSD Expert Says Government Should Inspect Source Code, Government Computer News, 6 March 1989, Ziff-Davis Publishing Company, New York, New York

29. Overview of Department of Defense Computer Security Guidelines, Information Security Volumes, 80-400-101/111, June 1985, DATAPRO Research Corporation, Delran, New Jersey

30. Planning for Defense Logistics Modernization, 1988, National Academy Press, Washington, D.C.

31. Report to the Chairman, Legislative and National Security Subcommittee, Committee on Government Operations, House of Representatives, Automated Information Systems, Schedule Delays and Cost Overruns Plague DoD Systems, United States General Accounting Office, May 1989, Washington, D.C.

32. Security Guidance is Urged for Govt. Computer Centers, February 6, 1989, Government Computer News, Ziff-Davis Publishing Company, New York, New York.

33. Security Requirements for Automated Information Systems (AISs), Department of Defense Directive 5200.28, 21 March 1988, Washington, D.C.

34. Selected Electronic Funds Transfer Issues - Privacy, Security andEquity, March 1982, Office of Technology Assessment, Washington, D.C.

35. Supply Security, Air Force Controls Need to Be Strengthened, B-230505, 12 February 1989, GAO/NSIAD-89-34, U.S. General Accounting Office, Washington, D.C.

36. The Paradoxical Proliferation of Paper, March-April 1988, Harvard Magazine, Harvard University Alumni Association, Harvard, Mass.

37. User's Needs Drive CALS Effort, Government Computer News, 15 May, 1989, Ziff-Davis Publishing Company, New York, New York

38. Viruses Pull Computer Underground Into Spotlight, 5 February 1989, The Washington Post, Washington, D.C.

39. Weak Links: ADP Security Deficiencies, Security Awareness Bulletin, September 1986/Number 5-86, Defense Investigative Service/Defense Security Institute, Richmond, Virginia

40. 101st Congress Deals With New Faces, Old Issues, Government Computer News, 23 January 1989, Ziff-Davis Publishing Company, New York, New York

41. 1988 Conceptual Functional Requirements, May 1988, Defense Logistics Agency, Alexandria, Virginia.